

# Calendar No. 181

112TH CONGRESS  
1ST SESSION

# S. 1151

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

---

## IN THE SENATE OF THE UNITED STATES

JUNE 7, 2011

Mr. LEAHY (for himself, Mr. SCHUMER, Mr. CARDIN, Mr. FRANKEN, and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

SEPTEMBER 22, 2011

Reported by Mr. LEAHY, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

---

## A BILL

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) **SHORT TITLE.**—This Act may be cited as the  
 3 “Personal Data Privacy and Security Act of 2011”.

4 (b) **TABLE OF CONTENTS.**—The table of contents of  
 5 this Act is as follows:

Sec. 1: Short title; table of contents.

Sec. 2: Findings.

Sec. 3: Definitions.

**TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND  
 OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY**

Sec. 101: Organized criminal activity in connection with unauthorized access to  
 personally identifiable information.

Sec. 102: Concealment of security breaches involving sensitive personally identi-  
 fiable information.

Sec. 103: Penalties for fraud and related activity in connection with computers.

**TITLE II—DATA BROKERS**

Sec. 201: Transparency and accuracy of data collection.

Sec. 202: Enforcement.

Sec. 203: Relation to State laws.

Sec. 204: Effective date.

**TITLE III—PRIVACY AND SECURITY OF PERSONALLY  
 IDENTIFIABLE INFORMATION**

**Subtitle A—A Data Privacy and Security Program**

Sec. 301: Purpose and applicability of data privacy and security program.

Sec. 302: Requirements for a personal data privacy and security program.

Sec. 303: Enforcement.

Sec. 304: Relation to other laws.

**Subtitle B—Security Breach Notification**

Sec. 311: Notice to individuals.

Sec. 312: Exemptions.

Sec. 313: Methods of notice.

Sec. 314: Content of notification.

Sec. 315: Coordination of notification with credit reporting agencies.

Sec. 316: Notice to law enforcement.

Sec. 317: Enforcement.

Sec. 318: Enforcement by State attorneys general.

Sec. 319: Effect on Federal and State law.

Sec. 320: Authorization of appropriations.

Sec. 321: Reporting on risk assessment exemptions.

Sec. 322: Effective date.

**TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL  
 DATA**

Sec. 401. General services administration review of contracts.

Sec. 402. Requirement to audit information security practices of contractors and third party business entities.

Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.

#### TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

Sec. 501. Budget compliance.

### 1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personally identifiable informa-  
4 tion are increasingly prime targets of hackers, iden-  
5 tity thieves, rogue employees, and other criminals,  
6 including organized and sophisticated criminal oper-  
7 ations;

8 (2) identity theft is a serious threat to the Na-  
9 tion's economic stability, homeland security, the de-  
10 velopment of e-commerce, and the privacy rights of  
11 Americans;

12 (3) over 9,300,000 individuals were victims of  
13 identity theft in America last year;

14 (4) security breaches are a serious threat to  
15 consumer confidence, homeland security, e-com-  
16 merce, and economic stability;

17 (5) it is important for business entities that  
18 own, use, or license personally identifiable informa-  
19 tion to adopt reasonable procedures to ensure the se-  
20 curity, privacy, and confidentiality of that personally  
21 identifiable information;

1           (6) individuals whose personal information has  
2           been compromised or who have been victims of iden-  
3           tity theft should receive the necessary information  
4           and assistance to mitigate their damages and to re-  
5           store the integrity of their personal information and  
6           identities;

7           (7) data brokers have assumed a significant  
8           role in providing identification, authentication, and  
9           screening services, and related data collection and  
10          analyses for commercial, nonprofit, and government  
11          operations;

12          (8) data misuse and use of inaccurate data have  
13          the potential to cause serious or irreparable harm to  
14          an individual's livelihood, privacy, and liberty and  
15          undermine efficient and effective business and gov-  
16          ernment operations;

17          (9) there is a need to ensure that data brokers  
18          conduct their operations in a manner that prioritizes  
19          fairness, transparency, accuracy, and respect for the  
20          privacy of consumers;

21          (10) government access to commercial data can  
22          potentially improve safety, law enforcement, and na-  
23          tional security; and

24          (11) because government use of commercial  
25          data containing personal information potentially af-

1       fects individual privacy, and law enforcement and  
2       national security operations, there is a need for Con-  
3       gress to exercise oversight over government use of  
4       commercial data.

5   **SEC. 3. DEFINITIONS.**

6       In this Act, the following definitions shall apply:

7           (1) AGENCY.—The term “agency” has the same  
8       meaning given such term in section 551 of title 5,  
9       United States Code.

10          (2) AFFILIATE.—The term “affiliate” means  
11       persons related by common ownership or by cor-  
12       porate control.

13          (3) BUSINESS ENTITY.—The term “business  
14       entity” means any organization, corporation, trust,  
15       partnership, sole proprietorship, unincorporated as-  
16       sociation, or venture established to make a profit, or  
17       nonprofit.

18          (4) IDENTITY THEFT.—The term “identity  
19       theft” means a violation of section 1028(a)(7) of  
20       title 18, United States Code.

21          (5) DATA BROKER.—The term “data broker”  
22       means a business entity which for monetary fees or  
23       dues regularly engages in the practice of collecting,  
24       transmitting, or providing access to sensitive person-  
25       ally identifiable information on more than 5,000 in-

dividuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to non-affiliated third parties on an interstate basis.

(6) DATA FURNISHER.—The term “data furnisher” means any agency, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or nonprofit that serves as a source of information for a data broker.

(7) ENCRYPTION.—The term “encryption”—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by a widely accepted standards setting body or, has been widely accepted as an effective industry practice which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(8) PERSONAL ELECTRONIC RECORD.—

(A) IN GENERAL.—The term “personal electronic record” means data associated with

an individual contained in a database,  
 networked or integrated databases, or other  
 data system that is provided by a data broker  
 to nonaffiliated third parties and includes per-  
 sonally identifiable information about that indi-  
 vidual.

(B) EXCLUSIONS.—The term “personal  
 electronic record” does not include—

(i) any data related to an individual’s  
 past purchases of consumer goods; or

(ii) any proprietary assessment or  
 evaluation of an individual or any propri-  
 etary assessment or evaluation of informa-  
 tion about an individual.

(9) PERSONALLY IDENTIFIABLE INFORMA-  
 TION.—The term “personally identifiable informa-  
 tion” means any information, or compilation of in-  
 formation, in electronic or digital form that is a  
 means of identification, as defined by section  
 1028(d)(7) of title 18, United State Code.

(10) PUBLIC RECORD SOURCE.—The term  
 “public record source” means the Congress, any  
 agency, any State or local government agency, the  
 government of the District of Columbia and govern-  
 ments of the territories or possessions of the United

1 States, and Federal, State or local courts, courts  
 2 martial and military commissions, that maintain  
 3 personally identifiable information in records avail-  
 4 able to the public.

5 ~~(11)~~ SECURITY BREACH.—

6 ~~(A)~~ IN GENERAL.—The term “security  
 7 breach” means compromise of the security, con-  
 8 fidentiality, or integrity of computerized data  
 9 through misrepresentation or actions—

10 (i) that result in, or that there is a  
 11 reasonable basis to conclude has resulted  
 12 in—

13 ~~(I)~~ the unauthorized acquisition  
 14 of sensitive personally identifiable in-  
 15 formation; and

16 ~~(II)~~ access to sensitive personally  
 17 identifiable information that is for an  
 18 unauthorized purpose, or in excess of  
 19 authorization; and

20 (ii) which present a significant risk of  
 21 harm or fraud to any individual.

22 ~~(B)~~ EXCLUSION.—The term “security  
 23 breach” does not include—

24 (i) a good faith acquisition of sensitive  
 25 personally identifiable information by a



business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or non-disclosure requirements; or

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States.

~~(12) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.~~—The term “sensitive personally identifiable information” means any information or compilation of information, in electronic or digital form that includes—

~~(A) an individual’s first and last name or first initial and last name in combination with any 1 of the following data elements:~~

~~(i) A non-truncated social security number, driver’s license number, passport number, or alien registration number.~~

~~(ii) Any 2 of the following:~~

1                   (I) Home address or telephone  
2                   number.

3                   (II) Mother's maiden name.

4                   (III) Month, day, and year of  
5                   birth.

6                   (iii) Unique biometric data such as a  
7                   finger print, voice print, a retina or iris  
8                   image, or any other unique physical rep-  
9                   resentation.

10                  (iv) A unique account identifier, elec-  
11                  tronic identification number, user name, or  
12                  routing code in combination with any asso-  
13                  ciated security code, access code, or pass-  
14                  word if the code or password is required  
15                  for an individual to obtain money, goods,  
16                  services, or any other thing of value; or

17                  (B) a financial account number or credit  
18                  or debit card number in combination with any  
19                  security code, access code, or password that is  
20                  required for an individual to obtain credit, with-  
21                  draw funds, or engage in a financial trans-  
22                  action.

1 **TITLE I—ENHANCING PUNISH-**  
 2 **MENT FOR IDENTITY THEFT**  
 3 **AND OTHER VIOLATIONS OF**  
 4 **DATA PRIVACY AND SECU-**  
 5 **RITY**

6 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**  
 7 **WITH UNAUTHORIZED ACCESS TO PERSON-**  
 8 **ALLY IDENTIFIABLE INFORMATION.**

9 Section 1961(1) of title 18, United States Code, is  
 10 amended by inserting “section 1030 (relating to fraud and  
 11 related activity in connection with computers) if the act  
 12 is a felony,” before “section 1084”.

13 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**  
 14 **ING SENSITIVE PERSONALLY IDENTIFIABLE**  
 15 **INFORMATION.**

16 (a) **IN GENERAL.**—Chapter 47 of title 18, United  
 17 States Code, is amended by adding at the end the fol-  
 18 lowing:

19 **“§ 1041. Concealment of security breaches involving**  
 20 **sensitive personally identifiable informa-**  
 21 **tion**

22 “(a) Whoever, having knowledge of a security breach  
 23 and having the obligation to provide notice of such breach  
 24 to individuals under title III of the Personal Data Privacy  
 25 and Security Act of 2011, and having not otherwise quali-

1 fined for an exemption from providing notice under section  
 2 312 of such Act, intentionally and willfully conceals the  
 3 fact of such security breach and which breach causes eco-  
 4 nomic damage to 1 or more persons, shall be fined under  
 5 this title or imprisoned not more than 5 years, or both.

6 “(b) For purposes of subsection (a), the term ‘person’  
 7 has the same meaning as in section 1030(e)(12) of title  
 8 18, United States Code.

9 “(c) Any person seeking an exemption under section  
 10 312(b) of the Personal Data Privacy and Security Act of  
 11 2011 shall be immune from prosecution under this section  
 12 if the United States Secret Service does not indicate, in  
 13 writing, that such notice be given under section 312(b)(3)  
 14 of such Act.”.

15 (b) CONFORMING AND TECHNICAL AMENDMENTS.—  
 16 The table of sections for chapter 47 of title 18, United  
 17 States Code, is amended by adding at the end the fol-  
 18 lowing:

“1041. Concealment of security breaches involving personally identifiable infor-  
 mation.”.

19 (c) ENFORCEMENT AUTHORITY.—

20 (1) IN GENERAL.—The United States Secret  
 21 Service shall have the authority to investigate of-  
 22 fenses under this section.

1           ~~(2)~~ NONEXCLUSIVITY.—The authority granted  
 2           in paragraph (1) shall not be exclusive of any exist-  
 3           ing authority held by any other Federal agency.

4   **SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY**  
 5                           **IN CONNECTION WITH COMPUTERS.**

6           Section 1030(c) of title 18, United States Code, is  
 7   amended—

8           ~~(1)~~ by inserting “or conspiracy” after “or an  
 9           attempt” each place it appears, except for paragraph  
 10          ~~(4)~~;

11          ~~(2)~~ in paragraph ~~(2)~~(B)—

12                  ~~(A)~~ in clause (i), by inserting “; or attempt  
 13                  or conspiracy or conspiracy to commit an of-  
 14                  fense,” after “the offense”;

15                  ~~(B)~~ in clause (ii), by inserting “; or at-  
 16                  tempt or conspiracy or conspiracy to commit an  
 17                  offense,” after “the offense”; and

18                  ~~(C)~~ in clause (iii), by inserting “(or, in the  
 19                  case of an attempted offense, would, if com-  
 20                  pleted, have obtained)” after “information ob-  
 21                  tained”; and

22          ~~(3)~~ in paragraph (4)—

23                  ~~(A)~~ in subparagraph (A)—

24                          ~~(i)~~ by striking clause (ii);

(ii) by striking “in the case of—” and all that follows through “an offense under subsection (a)(5)(B)” and inserting “in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(B)”;

(iii) by inserting “or conspiracy” after “if the offense”;

(iv) by redesignating subclauses (I) through (VI) as clauses (i) through (vi), respectively, and adjusting the margin accordingly; and

(v) in clause (vi), as so redesignated, by striking “; or” and inserting a semicolon;

(B) in subparagraph (B)—

(i) by striking clause (ii);

(ii) by striking “in the case of—” and all that follows through “an offense under subsection (a)(5)(A)” and inserting “in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(A)”;

(iii) by inserting “or conspiracy” after “if the offense”; and

1 (iv) by striking “; or” and inserting a  
 2 semicolon;

3 ~~(C)~~ in subparagraph ~~(C)~~—

4 (i) by striking clause (ii);

5 (ii) by striking “in the case of—” and  
 6 all that follows through “an offense or an  
 7 attempt to commit an offense” and insert-  
 8 ing “in the case of an offense; or an at-  
 9 tempt or conspiracy to commit an of-  
 10 fense,”; and

11 (iii) by striking “; or” and inserting a  
 12 semicolon;

13 ~~(D)~~ in subparagraph ~~(D)~~—

14 (i) by striking clause (ii);

15 (ii) by striking “in the case of—” and  
 16 all that follows through “an offense or an  
 17 attempt to commit an offense” and insert-  
 18 ing “in the case of an offense; or an at-  
 19 tempt or conspiracy to commit an of-  
 20 fense,”; and

21 (iii) by striking “; or” and inserting a  
 22 semicolon;

23 ~~(E)~~ in subparagraph ~~(E)~~, by inserting “or  
 24 conspires” after “offender attempts”;

(F) in subparagraph (F), by inserting “or conspires” after “offender attempts”; and

(G) in subparagraph (G)(ii), by inserting “or conspiracy” after “an attempt”.

## **TITLE II—DATA BROKERS**

### **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.**

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any product or service offered to third parties that allows access or use of personally identifiable information.

(b) LIMITATION.—Notwithstanding any other provision of this section, this section shall not apply to—

(1) any product or service offered by a data broker engaging in interstate commerce where such product or service is currently subject to, and in compliance with, access and accuracy protections similar to those under subsections (c) through (e) of this section under the Fair Credit Reporting Act (Public Law 91–508);

(2) any data broker that is subject to regulation under the Gramm-Leach-Bliley Act (Public Law 106–102);

(3) any data broker currently subject to and in compliance with the data security requirements for



1 such entities under the Health Insurance Portability  
2 and Accountability Act (Public Law 104–191), and  
3 its implementing regulations;

4 (4) any data broker subject to, and in compli-  
5 ance with, the privacy and data security require-  
6 ments under sections 13401 and 13404 of division  
7 A of the American Reinvestment and Recovery Act  
8 of 2009 (42 U.S.C. 17931 and 17934) and imple-  
9 menting regulations promulgated under such sec-  
10 tions;

11 (5) information in a personal electronic record  
12 that—

13 (A) the data broker has identified as inae-  
14 curate, but maintains for the purpose of aiding  
15 the data broker in preventing inaccurate infor-  
16 mation from entering an individual’s personal  
17 electronic record; and

18 (B) is not maintained primarily for the  
19 purpose of transmitting or otherwise providing  
20 that information, or assessments based on that  
21 information, to nonaffiliated third parties;

22 (6) information concerning proprietary meth-  
23 odologies, techniques, scores, or algorithms relating  
24 to fraud prevention not normally provided to third  
25 parties in the ordinary course of business; and

1           (7) information that is used for legitimate gov-  
 2           ernmental or fraud prevention purposes that would  
 3           be compromised by disclosure to the individual.

4           (c) DISCLOSURES TO INDIVIDUALS.—

5           (1) IN GENERAL.—A data broker shall, upon  
 6           the request of an individual, disclose to such indi-  
 7           vidual for a reasonable fee all personal electronic  
 8           records pertaining to that individual maintained or  
 9           accessed by the data broker specifically for disclo-  
 10          sure to third parties that request information on  
 11          that individual in the ordinary course of business in  
 12          the databases or systems of the data broker at the  
 13          time of such request.

14          (2) INFORMATION ON HOW TO CORRECT INAC-  
 15          CURACIES.—The disclosures required under para-  
 16          graph (1) shall also include guidance to individuals  
 17          on procedures for correcting inaccuracies.

18          (d) DISCLOSURE TO INDIVIDUALS OF ADVERSE AC-  
 19          TIONS TAKEN BY THIRD PARTIES.—

20          (1) IN GENERAL.—If a person takes any ad-  
 21          verse action with respect to any individual that is  
 22          based, in whole or in part, on any information con-  
 23          tained in a personal electronic record, the person, at  
 24          no cost to the affected individual, shall provide—

1           (A) written or electronic notice of the ad-  
 2           verse action to the individual;

3           (B) to the individual, in writing or elec-  
 4           tronically, the name, address, and telephone  
 5           number of the data broker (including a toll-free  
 6           telephone number established by the data  
 7           broker, if the data broker complies and main-  
 8           tains data on individuals on a nationwide basis)  
 9           that furnished the information to the person;

10          (C) a copy of the information such person  
 11          obtained from the data broker; and

12          (D) information to the individual on the  
 13          procedures for correcting any inaccuracies in  
 14          such information.

15          (2) ACCEPTED METHODS OF NOTICE.—A per-  
 16          son shall be in compliance with the notice require-  
 17          ments under paragraph (1) if such person provides  
 18          written or electronic notice in the same manner and  
 19          using the same methods as are required under sec-  
 20          tion 313(1) of this Act.

21          (c) ACCURACY RESOLUTION PROCESS.—

22               (1) INFORMATION FROM A PUBLIC RECORD OR  
 23               LICENSOR.—

24                   (A) IN GENERAL.—If an individual notifies  
 25                   a data broker of a dispute as to the complete-

ness or accuracy of information disclosed to such individual under subsection (c) that is obtained from a public record source or a license agreement, such data broker shall determine within 30 days whether the information in its system accurately and completely records the information available from the licensor or public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems does not accurately and completely record the information available from a public record source or licensor, the data broker shall—

(i) correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) provide such individual with the contact information of the public record or licensor.

(2) INFORMATION NOT FROM A PUBLIC RECORD SOURCE OR LICENSOR.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information not from a public record or licensor that was disclosed to the individual under

1 subsection (c), the data broker shall, within 30 days  
2 of receiving notice of such dispute—

3 (A) review and consider free of charge any  
4 information submitted by such individual that is  
5 relevant to the completeness or accuracy of the  
6 disputed information; and

7 (B) correct any information found to be in-  
8 complete or inaccurate and provide notice to  
9 such individual of whether and what informa-  
10 tion was corrected, if any.

11 (3) EXTENSION OF REVIEW PERIOD.—The 30-  
12 day period described in paragraph (1) may be ex-  
13 tended for not more than 30 additional days if a  
14 data broker receives information from the individual  
15 during the initial 30-day period that is relevant to  
16 the completeness or accuracy of any disputed infor-  
17 mation.

18 (4) NOTICE IDENTIFYING THE DATA FUR-  
19 NISHER.—If the completeness or accuracy of any in-  
20 formation not from a public record source or licensor  
21 that was disclosed to an individual under subsection  
22 (c) is disputed by such individual, the data broker  
23 shall provide, upon the request of such individual,  
24 the contact information of any data furnisher that  
25 provided the disputed information.

1           ~~(5) DETERMINATION THAT DISPUTE IS FRIVO-~~  
 2           ~~LOUS OR IRRELEVANT.—~~

3           ~~(A) IN GENERAL.—~~Notwithstanding para-  
 4           graphs ~~(1)~~ through ~~(3)~~, a data broker may de-  
 5           cline to investigate or terminate a review of in-  
 6           formation disputed by an individual under those  
 7           paragraphs if the data broker reasonably deter-  
 8           mines that the dispute by the individual is friv-  
 9           olous or intended to perpetrate fraud.

10           ~~(B) NOTICE.—~~A data broker shall notify  
 11           an individual of a determination under subpara-  
 12           graph ~~(A)~~ within a reasonable time by any  
 13           means available to such data broker.

14   **SEC. 202. ENFORCEMENT.**

15           ~~(a) CIVIL PENALTIES.—~~

16           ~~(1) PENALTIES.—~~Any data broker that violates  
 17           the provisions of section 201 shall be subject to civil  
 18           penalties of not more than \$1,000 per violation per  
 19           day while such violations persist, up to a maximum  
 20           of \$250,000 per violation.

21           ~~(2) INTENTIONAL OR WILLFUL VIOLATION.—~~A  
 22           data broker that intentionally or willfully violates the  
 23           provisions of section 201 shall be subject to addi-  
 24           tional penalties in the amount of \$1,000 per viola-

1       tion per day, to a maximum of an additional  
2       \$250,000 per violation, while such violations persist.

3           ~~(3) EQUITABLE RELIEF.~~—A data broker en-  
4       gaged in interstate commerce that violates this sec-  
5       tion may be enjoined from further violations by a  
6       court of competent jurisdiction.

7           ~~(4) OTHER RIGHTS AND REMEDIES.~~—The  
8       rights and remedies available under this subsection  
9       are cumulative and shall not affect any other rights  
10      and remedies available under law.

11      ~~(b) FEDERAL TRADE COMMISSION AUTHORITY.~~—  
12   Any data broker shall have the provisions of this title en-  
13   forced against it by the Federal Trade Commission.

14      ~~(c) STATE ENFORCEMENT.~~—

15           ~~(1) CIVIL ACTIONS.~~—In any case in which the  
16      attorney general of a State or any State or local law  
17      enforcement agency authorized by the State attorney  
18      general or by State statute to prosecute violations of  
19      consumer protection law, has reason to believe that  
20      an interest of the residents of that State has been  
21      or is threatened or adversely affected by the acts or  
22      practices of a data broker that violate this title, the  
23      State may bring a civil action on behalf of the resi-  
24      dents of that State in a district court of the United

1 States of appropriate jurisdiction, or any other court  
2 of competent jurisdiction, to—

3 (A) enjoin that act or practice;

4 (B) enforce compliance with this title; or

5 (C) obtain civil penalties of not more than  
6 \$1,000 per violation per day while such viola-  
7 tions persist, up to a maximum of \$250,000 per  
8 violation.

9 (2) NOTICE.—

10 (A) IN GENERAL.—Before filing an action  
11 under this subsection, the attorney general of  
12 the State involved shall provide to the Federal  
13 Trade Commission—

14 (i) a written notice of that action; and

15 (ii) a copy of the complaint for that  
16 action.

17 (B) EXCEPTION.—Subparagraph (A) shall  
18 not apply with respect to the filing of an action  
19 by an attorney general of a State under this  
20 subsection, if the attorney general of a State  
21 determines that it is not feasible to provide the  
22 notice described in subparagraph (A) before the  
23 filing of the action.

24 (C) NOTIFICATION WHEN PRACTICABLE.—

25 In an action described under subparagraph (B),



the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

~~(3) FEDERAL TRADE COMMISSION AUTHORITY.~~—Upon receiving notice under paragraph ~~(2)~~, the Federal Trade Commission shall have the right to—

~~(A)~~ move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph ~~(4)~~;

~~(B)~~ intervene in an action brought under paragraph ~~(1)~~; and

~~(C)~~ file petitions for appeal.

~~(4) PENDING PROCEEDINGS.~~—If the Federal Trade Commission has instituted a proceeding or civil action for a violation of this title, no attorney general of a State may, during the pendency of such proceeding or civil action, bring an action under this subsection against any defendant named in such civil action for any violation that is alleged in that civil action.

~~(5) RULE OF CONSTRUCTION.~~—For purposes of bringing any civil action under paragraph ~~(1)~~, nothing in this title shall be construed to prevent an at-

1       torney general of a State from exercising the powers  
 2       conferred on the attorney general by the laws of that  
 3       State to—

4               (A) conduct investigations;

5               (B) administer oaths and affirmations; or

6               (C) compel the attendance of witnesses or  
 7       the production of documentary and other evi-  
 8       dence.

9       ~~(6) VENUE; SERVICE OF PROCESS.—~~

10           (A) ~~VENUE.—~~Any action brought under  
 11       this subsection may be brought in the district  
 12       court of the United States that meets applicable  
 13       requirements relating to venue under section  
 14       1391 of title 28, United States Code.

15           (B) ~~SERVICE OF PROCESS.—~~In an action  
 16       brought under this subsection, process may be  
 17       served in any district in which the defendant—

18               (i) is an inhabitant; or

19               (ii) may be found.

20       ~~(d) NO PRIVATE CAUSE OF ACTION.—~~Nothing in  
 21       this title establishes a private cause of action against a  
 22       data broker for violation of any provision of this title.

23       **SEC. 203. RELATION TO STATE LAWS.**

24       No requirement or prohibition may be imposed under  
 25       the laws of any State with respect to any subject matter

1 regulated under section 201, relating to individual access  
 2 to, and correction of, personal electronic records held by  
 3 data brokers.

4 **SEC. 204. EFFECTIVE DATE.**

5 This title shall take effect 180 days after the date  
 6 of enactment of this Act.

7 **TITLE III—PRIVACY AND SECU-**  
 8 **RITY OF PERSONALLY IDEN-**  
 9 **TIFIABLE INFORMATION**

10 **Subtitle A—A Data Privacy and**  
 11 **Security Program**

12 **SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY**  
 13 **AND SECURITY PROGRAM.**

14 (a) **PURPOSE.**—The purpose of this subtitle is to en-  
 15 sure standards for developing and implementing adminis-  
 16 trative, technical, and physical safeguards to protect the  
 17 security of sensitive personally identifiable information.

18 (b) **IN GENERAL.**—A business entity engaging in  
 19 interstate commerce that involves collecting, accessing,  
 20 transmitting, using, storing, or disposing of sensitive per-  
 21 sonally identifiable information in electronic or digital  
 22 form on 10,000 or more United States persons is subject  
 23 to the requirements for a data privacy and security pro-  
 24 gram under section 302 for protecting sensitive personally  
 25 identifiable information.

1       (e) ~~LIMITATIONS.~~—Notwithstanding any other obli-  
 2       gation under this subtitle, this subtitle does not apply to:

3               (1) ~~FINANCIAL INSTITUTIONS.~~—Financial insti-  
 4       tutions—

5                       (A) subject to the data security require-  
 6                       ments and implementing regulations under the  
 7                       Gramm-Leach-Bliley Act (~~15 U.S.C. 6801 et~~  
 8                       seq.); and

9                       (B) subject to—

10                               (i) examinations for compliance with  
 11                               the requirements of this Act by a Federal  
 12                               Functional Regulator or State Insurance  
 13                               Authority (as those terms are defined in  
 14                               section 509 of the Gramm-Leach-Bliley  
 15                               Act (~~15 U.S.C. 6809~~)); or

16                               (ii) compliance with part 314 of title  
 17                               16, Code of Federal Regulations.

18       (2) ~~HIPPA REGULATED ENTITIES.~~—

19                       (A) ~~COVERED ENTITIES.~~—Covered entities  
 20                       subject to the Health Insurance Portability and  
 21                       Accountability Act of 1996 (~~42 U.S.C. 1301 et~~  
 22                       seq.); including the data security requirements  
 23                       and implementing regulations of that Act.

1           ~~(B) BUSINESS ENTITIES.—A Business en-~~  
 2           ~~tity shall be deemed in compliance with this Act~~  
 3           ~~if the business entity—~~

4                     ~~(i) is acting as a business associate,~~  
 5                     ~~as that term is defined under the Health~~  
 6                     ~~Insurance Portability and Accountability~~  
 7                     ~~Act of 1996 (42 U.S.C. 1301 et seq.) and~~  
 8                     ~~is in compliance with the requirements im-~~  
 9                     ~~posed under that Act and implementing~~  
 10                    ~~regulations promulgated under that Act;~~  
 11                    ~~and~~

12                   ~~(ii) is subject to, and currently in~~  
 13                    ~~compliance, with the privacy and data se-~~  
 14                    ~~curity requirements under sections 13401~~  
 15                    ~~and 13404 of division A of the American~~  
 16                    ~~Reinvestment and Recovery Act of 2009~~  
 17                    ~~(42 U.S.C. 17931 and 17934) and imple-~~  
 18                    ~~menting regulations promulgated under~~  
 19                    ~~such sections.~~

20           ~~(3) PUBLIC RECORDS.—Public records not oth-~~  
 21           ~~erwise subject to a confidentiality or nondisclosure~~  
 22           ~~requirement, or information obtained from a news~~  
 23           ~~report or periodical.~~

24           ~~(d) SAFE HARBORS.—~~

1           (1) ~~IN GENERAL.~~—A business entity shall be  
 2       deemed in compliance with the privacy and security  
 3       program requirements under section 302 if the busi-  
 4       ness entity complies with or provides protection  
 5       equal to industry standards or standards widely ac-  
 6       cepted as an effective industry practice, as identified  
 7       by the Federal Trade Commission, that are applica-  
 8       ble to the type of sensitive personally identifiable in-  
 9       formation involved in the ordinary course of business  
 10      of such business entity.

11          (2) ~~LIMITATION.~~—Nothing in this subsection  
 12      shall be construed to permit, and nothing does per-  
 13      mit, the Federal Trade Commission to issue regula-  
 14      tions requiring, or according greater legal status to,  
 15      the implementation of or application of a specific  
 16      technology or technological specifications for meeting  
 17      the requirements of this title.

18 **SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**  
 19 **AND SECURITY PROGRAM.**

20          (a) ~~PERSONAL DATA PRIVACY AND SECURITY PRO-~~  
 21 ~~GRAM.~~—A business entity subject to this subtitle shall  
 22      comply with the following safeguards and any other ad-  
 23      ministrative, technical, or physical safeguards identified by  
 24      the Federal Trade Commission in a rulemaking process  
 25      pursuant to section 553 of title 5, United States Code,

1 for the protection of sensitive personally identifiable infor-  
2 mation:

3           ~~(1) SCOPE.~~—A business entity shall implement  
4 a comprehensive personal data privacy and security  
5 program that includes administrative, technical, and  
6 physical safeguards appropriate to the size and com-  
7 plexity of the business entity and the nature and  
8 scope of its activities.

9           ~~(2) DESIGN.~~—The personal data privacy and  
10 security program shall be designed to—

11               ~~(A)~~ ensure the privacy, security, and con-  
12 fidentiality of sensitive personally identifying in-  
13 formation;

14               ~~(B)~~ protect against any anticipated  
15 vulnerabilities to the privacy, security, or integ-  
16 rity of sensitive personally identifying informa-  
17 tion; and

18               ~~(C)~~ protect against unauthorized access to  
19 use of sensitive personally identifying informa-  
20 tion that could create a significant risk of harm  
21 or fraud to any individual.

22           ~~(3) RISK ASSESSMENT.~~—A business entity  
23 shall—

24               ~~(A)~~ identify reasonably foreseeable internal  
25 and external vulnerabilities that could result in

1 unauthorized access, disclosure, use, or alter-  
2 ation of sensitive personally identifiable infor-  
3 mation or systems containing sensitive person-  
4 ally identifiable information;

5 (B) assess the likelihood of and potential  
6 damage from unauthorized access, disclosure,  
7 use, or alteration of sensitive personally identifi-  
8 able information;

9 (C) assess the sufficiency of its policies,  
10 technologies, and safeguards in place to control  
11 and minimize risks from unauthorized access,  
12 disclosure, use, or alteration of sensitive person-  
13 ally identifiable information; and

14 (D) assess the vulnerability of sensitive  
15 personally identifiable information during de-  
16 struction and disposal of such information, in-  
17 cluding through the disposal or retirement of  
18 hardware.

19 (4) RISK MANAGEMENT AND CONTROL.—Each  
20 business entity shall—

21 (A) design its personal data privacy and  
22 security program to control the risks identified  
23 under paragraph (3); and

24 (B) adopt measures commensurate with  
25 the sensitivity of the data as well as the size,



1 complexity, and scope of the activities of the  
2 business entity that—

3 (i) control access to systems and fa-  
4 cilities containing sensitive personally iden-  
5 tifiable information, including controls to  
6 authenticate and permit access only to au-  
7 thorized individuals;

8 (ii) detect, record, and preserve infor-  
9 mation relevant to actual and attempted  
10 fraudulent, unlawful, or unauthorized ac-  
11 cess, disclosure, use, or alteration of sen-  
12 sitive personally identifiable information,  
13 including by employees and other individ-  
14 uals otherwise authorized to have access;

15 (iii) protect sensitive personally identi-  
16 fiable information during use, trans-  
17 mission, storage, and disposal by  
18 encryption, redaction, or access controls  
19 that are widely accepted as an effective in-  
20 dustry practice or industry standard, or  
21 other reasonable means (including as di-  
22 rected for disposal of records under section  
23 628 of the Fair Credit Reporting Act (15  
24 U.S.C. 1681w) and the implementing regu-  
25 lations of such Act as set forth in section

1 682 of title 16, Code of Federal Regula-  
2 tions);

3 (iv) ensure that sensitive personally  
4 identifiable information is properly de-  
5 stroyed and disposed of, including during  
6 the destruction of computers, diskettes,  
7 and other electronic media that contain  
8 sensitive personally identifiable informa-  
9 tion;

10 (v) trace access to records containing  
11 sensitive personally identifiable information  
12 so that the business entity can determine  
13 who accessed or acquired such sensitive  
14 personally identifiable information per-  
15 taining to specific individuals; and

16 (vi) ensure that no third party or cus-  
17 tomer of the business entity is authorized  
18 to access or acquire sensitive personally  
19 identifiable information without the busi-  
20 ness entity first performing sufficient due  
21 diligence to ascertain, with reasonable cer-  
22 tainty, that such information is being  
23 sought for a valid legal purpose.

24 (b) TRAINING.—Each business entity subject to this  
25 subtitle shall take steps to ensure employee training and

1 supervision for implementation of the data security pro-  
2 gram of the business entity.

3 ~~(c) VULNERABILITY TESTING.—~~

4 ~~(1) IN GENERAL.—~~Each business entity subject  
5 to this subtitle shall take steps to ensure regular  
6 testing of key controls, systems, and procedures of  
7 the personal data privacy and security program to  
8 detect, prevent, and respond to attacks or intrusions,  
9 or other system failures.

10 ~~(2) FREQUENCY.—~~The frequency and nature of  
11 the tests required under paragraph (1) shall be de-  
12 termined by the risk assessment of the business enti-  
13 ty under subsection (a)(3).

14 ~~(d) RELATIONSHIP TO SERVICE PROVIDERS.—~~In the  
15 event a business entity subject to this subtitle engages  
16 service providers not subject to this subtitle, such business  
17 entity shall—

18 ~~(1)~~ exercise appropriate due diligence in select-  
19 ing those service providers for responsibilities related  
20 to sensitive personally identifiable information, and  
21 take reasonable steps to select and retain service  
22 providers that are capable of maintaining appro-  
23 priate safeguards for the security, privacy, and in-  
24 tegrity of the sensitive personally identifiable infor-  
25 mation at issue; and

1           (2) require those service providers by contract  
 2           to implement and maintain appropriate measures de-  
 3           signed to meet the objectives and requirements gov-  
 4           erning entities subject to section 301, this section,  
 5           and subtitle B.

6           (c) PERIODIC ASSESSMENT AND PERSONAL DATA  
 7           PRIVACY AND SECURITY MODERNIZATION.—Each busi-  
 8           ness entity subject to this subtitle shall on a regular basis  
 9           monitor, evaluate, and adjust, as appropriate its data pri-  
 10          vacy and security program in light of any relevant changes  
 11          in—

12                 (1) technology;

13                 (2) the sensitivity of personally identifiable in-  
 14          formation;

15                 (3) internal or external threats to personally  
 16          identifiable information; and

17                 (4) the changing business arrangements of the  
 18          business entity, such as—

19                         (A) mergers and acquisitions;

20                         (B) alliances and joint ventures;

21                         (C) outsourcing arrangements;

22                         (D) bankruptcy; and

23                         (E) changes to sensitive personally identifi-  
 24          able information systems.

1       (f) IMPLEMENTATION TIMELINE.—Not later than 1  
 2 year after the date of enactment of this Act, a business  
 3 entity subject to the provisions of this subtitle shall imple-  
 4 ment a data privacy and security program pursuant to this  
 5 subtitle.

6 **SEC. 303. ENFORCEMENT.**

7       (a) CIVIL PENALTIES.—

8           (1) IN GENERAL.—Any business entity that vio-  
 9 lates the provisions of sections 301 or 302 shall be  
 10 subject to civil penalties of not more than \$5,000  
 11 per violation per day while such a violation exists,  
 12 with a maximum of \$500,000 per violation.

13          (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
 14 business entity that intentionally or willfully violates  
 15 the provisions of sections 301 or 302 shall be subject  
 16 to additional penalties in the amount of \$5,000 per  
 17 violation per day while such a violation exists, with  
 18 a maximum of an additional \$500,000 per violation.

19          (3) EQUITABLE RELIEF.—A business entity en-  
 20 gaged in interstate commerce that violates this sec-  
 21 tion may be enjoined from further violations by a  
 22 court of competent jurisdiction.

23          (4) OTHER RIGHTS AND REMEDIES.—The  
 24 rights and remedies available under this section are

1 cumulative and shall not affect any other rights and  
 2 remedies available under law.

3 ~~(b) FEDERAL TRADE COMMISSION AUTHORITY.—~~

4 Any business entity shall have the provisions of this sub-  
 5 title enforced against it by the Federal Trade Commission.

6 ~~(c) STATE ENFORCEMENT.—~~

7 ~~(1) CIVIL ACTIONS.—~~In any case in which the  
 8 attorney general of a State or any State or local law  
 9 enforcement agency authorized by the State attorney  
 10 general or by State statute to prosecute violations of  
 11 consumer protection law, has reason to believe that  
 12 an interest of the residents of that State has been  
 13 or is threatened or adversely affected by the acts or  
 14 practices of a business entity that violate this sub-  
 15 title, the State may bring a civil action on behalf of  
 16 the residents of that State in a district court of the  
 17 United States of appropriate jurisdiction, or any  
 18 other court of competent jurisdiction, to—

19 ~~(A) enjoin that act or practice;~~

20 ~~(B) enforce compliance with this subtitle;~~

21 or

22 ~~(C) obtain civil penalties of not more than~~  
 23 ~~\$5,000 per violation per day while such viola-~~  
 24 ~~tions persist, up to a maximum of \$500,000 per~~  
 25 ~~violation.~~

1           (2) NOTICE.—

2           (A) IN GENERAL.—Before filing an action  
3           under this subsection, the attorney general of  
4           the State involved shall provide to the Federal  
5           Trade Commission—

6                   (i) a written notice of that action; and

7                   (ii) a copy of the complaint for that  
8           action.

9           (B) EXCEPTION.—Subparagraph (A) shall  
10          not apply with respect to the filing of an action  
11          by an attorney general of a State under this  
12          subsection, if the attorney general of a State  
13          determines that it is not feasible to provide the  
14          notice described in this subparagraph before the  
15          filing of the action.

16          (C) NOTIFICATION WHEN PRACTICABLE.—

17          In an action described under subparagraph (B),  
18          the attorney general of a State shall provide the  
19          written notice and the copy of the complaint to  
20          the Federal Trade Commission as soon after  
21          the filing of the complaint as practicable.

22          (3) FEDERAL TRADE COMMISSION AUTHOR-

23          ITY.—Upon receiving notice under paragraph (2),  
24          the Federal Trade Commission shall have the right  
25          to—

1           (A) move to stay the action, pending the  
2           final disposition of a pending Federal pro-  
3           ceeding or action as described in paragraph (4);

4           (B) intervene in an action brought under  
5           paragraph (1); and

6           (C) file petitions for appeal.

7           (4) PENDING PROCEEDINGS.—If the Federal  
8           Trade Commission has instituted a proceeding or ac-  
9           tion for a violation of this subtitle or any regulations  
10          thereunder, no attorney general of a State may, dur-  
11          ing the pendency of such proceeding or action, bring  
12          an action under this subsection against any defend-  
13          ant named in such criminal proceeding or civil ac-  
14          tion for any violation that is alleged in that pro-  
15          ceeding or action.

16          (5) RULE OF CONSTRUCTION.—For purposes of  
17          bringing any civil action under paragraph (1) noth-  
18          ing in this subtitle shall be construed to prevent an  
19          attorney general of a State from exercising the pow-  
20          ers conferred on the attorney general by the laws of  
21          that State to—

22               (A) conduct investigations;

23               (B) administer oaths and affirmations; or



1           (C) compel the attendance of witnesses or  
 2           the production of documentary and other evi-  
 3           dence.

4           (6) VENUE; SERVICE OF PROCESS.—

5           (A) VENUE.—Any action brought under  
 6           this subsection may be brought in the district  
 7           court of the United States that meets applicable  
 8           requirements relating to venue under section  
 9           1391 of title 28, United States Code.

10          (B) SERVICE OF PROCESS.—In an action  
 11          brought under this subsection, process may be  
 12          served in any district in which the defendant—

13               (i) is an inhabitant; or

14               (ii) may be found.

15          (d) NO PRIVATE CAUSE OF ACTION.—Nothing in  
 16          this subtitle establishes a private cause of action against  
 17          a business entity for violation of any provision of this sub-  
 18          title.

19       **SEC. 304. RELATION TO OTHER LAWS.**

20          (a) IN GENERAL.—No State may require any busi-  
 21          ness entity subject to this subtitle to comply with any re-  
 22          quirements with respect to administrative, technical, and  
 23          physical safeguards for the protection of sensitive person-  
 24          ally identifying information.

1 (b) LIMITATIONS.—Nothing in this subtitle shall be  
 2 construed to modify, limit, or supersede the operation of  
 3 the Gramm-Leach-Bliley Act or its implementing regula-  
 4 tions, including those adopted or enforced by States.

## 5 **Subtitle B—Security Breach** 6 **Notification**

### 7 **SEC. 311. NOTICE TO INDIVIDUALS.**

8 (a) IN GENERAL.—Any agency, or business entity en-  
 9 gaged in interstate commerce, that uses, accesses, trans-  
 10 mits, stores, disposes of or collects sensitive personally  
 11 identifiable information shall, following the discovery of a  
 12 security breach of such information, notify any resident  
 13 of the United States whose sensitive personally identifiable  
 14 information has been, or is reasonably believed to have  
 15 been, accessed, or acquired.

### 16 (b) OBLIGATION OF OWNER OR LICENSEE.—

17 (1) NOTICE TO OWNER OR LICENSEE.—Any  
 18 agency, or business entity engaged in interstate com-  
 19 merce, that uses, accesses, transmits, stores, dis-  
 20 poses of, or collects sensitive personally identifiable  
 21 information that the agency or business entity does  
 22 not own or license shall notify the owner or licensee  
 23 of the information following the discovery of a secu-  
 24 rity breach involving such information.

1           ~~(2) NOTICE BY OWNER, LICENSEE OR OTHER~~  
 2           ~~DESIGNATED THIRD PARTY.—~~Nothing in this sub-  
 3           title shall prevent or abrogate an agreement between  
 4           an agency or business entity required to give notice  
 5           under this section and a designated third party, in-  
 6           cluding an owner or licensee of the sensitive person-  
 7           ally identifiable information subject to the security  
 8           breach, to provide the notifications required under  
 9           subsection (a).

10           ~~(3) BUSINESS ENTITY RELIEVED FROM GIVING~~  
 11           ~~NOTICE.—~~A business entity obligated to give notice  
 12           under subsection (a) shall be relieved of such obliga-  
 13           tion if an owner or licensee of the sensitive person-  
 14           ally identifiable information subject to the security  
 15           breach, or other designated third party, provides  
 16           such notification.

17           ~~(c) TIMELINESS OF NOTIFICATION.—~~

18           ~~(1) IN GENERAL.—~~All notifications required  
 19           under this section shall be made without unreason-  
 20           able delay following the discovery by the agency or  
 21           business entity of a security breach.

22           ~~(2) REASONABLE DELAY.—~~Reasonable delay  
 23           under this subsection may include any time nec-  
 24           essary to determine the scope of the security breach,  
 25           prevent further disclosures, conduct the risk assess-

1        ment described in section 302(a)(3), and restore the  
 2        reasonable integrity of the data system and provide  
 3        notice to law enforcement when required.

4            ~~(3) BURDEN OF PRODUCTION.~~—The agency,  
 5        business entity, owner, or licensee required to pro-  
 6        vide notice under this subtitle shall, upon the re-  
 7        quest of the Attorney General, provide records or  
 8        other evidence of the notifications required under  
 9        this subtitle, including to the extent applicable, the  
 10       reasons for any delay of notification.

11       ~~(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW~~  
 12 ~~ENFORCEMENT PURPOSES.—~~

13            ~~(1) IN GENERAL.~~—If a Federal law enforce-  
 14        ment or intelligence agency determines that the noti-  
 15        fication required under this section would impede a  
 16        criminal investigation, such notification shall be de-  
 17        layed upon written notice from such Federal law en-  
 18        forcement or intelligence agency to the agency or  
 19        business entity that experienced the breach.

20            ~~(2) EXTENDED DELAY OF NOTIFICATION.~~—If  
 21        the notification required under subsection (a) is de-  
 22        layed pursuant to paragraph (1), an agency or busi-  
 23        ness entity shall give notice 30 days after the day  
 24        such law enforcement delay was invoked unless a  
 25        Federal law enforcement or intelligence agency pro-

1       vides written notification that further delay is nec-  
2       essary.

3           ~~(3) LAW ENFORCEMENT IMMUNITY.—~~No cause  
4       of action shall lie in any court against any law en-  
5       forcement agency for acts relating to the delay of  
6       notification for law enforcement purposes under this  
7       subtitle.

8   **SEC. 312. EXEMPTIONS.**

9       ~~(a) EXEMPTION FOR NATIONAL SECURITY AND LAW~~  
10   ~~ENFORCEMENT.—~~

11           ~~(1) IN GENERAL.—~~Section 311 shall not apply  
12       to an agency or business entity if the agency or busi-  
13       ness entity certifies, in writing, that notification of  
14       the security breach as required by section 311 rea-  
15       sonably could be expected to—

16                   ~~(A) cause damage to the national security;~~  
17                   ~~or~~

18                   ~~(B) hinder a law enforcement investigation~~  
19                   ~~or the ability of the agency to conduct law en-~~  
20                   ~~forcement investigations.~~

21           ~~(2) LIMITS ON CERTIFICATIONS.—~~An agency or  
22       business entity may not execute a certification under  
23       paragraph (1) to—

24                   ~~(A) conceal violations of law, inefficiency,~~  
25                   ~~or administrative error;~~

1           ~~(B)~~ prevent embarrassment to a business  
2           entity, organization, or agency; or

3           ~~(C)~~ restrain competition.

4           ~~(3)~~ NOTICE.—In every case in which an agency  
5           or business agency issues a certification under para-  
6           graph ~~(1)~~, the certification, accompanied by a de-  
7           scription of the factual basis for the certification,  
8           shall be immediately provided to the United States  
9           Secret Service and the Federal Bureau of Investiga-  
10          tion.

11          ~~(4)~~ SECRET SERVICE AND FBI REVIEW OF CER-  
12          TIFICATIONS.—

13               ~~(A)~~ IN GENERAL.—The United States Se-  
14               cret Service or the Federal Bureau of Investiga-  
15               tion may review a certification provided by an  
16               agency under paragraph ~~(3)~~, and shall review a  
17               certification provided by a business entity under  
18               paragraph ~~(3)~~, to determine whether an exemp-  
19               tion under paragraph ~~(1)~~ is merited. Such re-  
20               view shall be completed not later than 10 busi-  
21               ness days after the date of receipt of the certifi-  
22               cation, except as provided in paragraph ~~(5)~~(C).

23               ~~(B)~~ NOTICE.—Upon completing a review  
24               under subparagraph ~~(A)~~ the United States Se-  
25               cret Service or the Federal Bureau of Investiga-

tion shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service or the Federal Bureau of Investigation determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE AND FBI.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service or the Federal Bureau of Investigation may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

1           (C) ~~TIMING.~~—If the United States Secret  
 2           Service or the Federal Bureau of Investigation  
 3           requests additional information under subpara-  
 4           graph (A), the United States Secret Service or  
 5           the Federal Bureau of Investigation shall notify  
 6           the agency or business entity not later than 10  
 7           business days after the date of receipt of the  
 8           additional information whether an exemption  
 9           under paragraph (1) is merited.

10       (b) ~~SAFE HARBOR.~~—An agency or business entity  
 11       will be exempt from the notice requirements under section  
 12       311, if—

13           (1) a risk assessment concludes that—

14           (A) there is no significant risk that a secu-  
 15           rity breach has resulted in, or will result in,  
 16           harm to the individuals whose sensitive person-  
 17           ally identifiable information was subject to the  
 18           security breach, with the encryption of such in-  
 19           formation establishing a presumption that no  
 20           significant risk exists; or

21           (B) there is no significant risk that a secu-  
 22           rity breach has resulted in, or will result in,  
 23           harm to the individuals whose sensitive person-  
 24           ally identifiable information was subject to the  
 25           security breach, with the rendering of such sen-



sitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, establishing a presumption that no significant risk exists;

(2) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the United States Secret Service or the Federal Bureau of Investigation, the agency or business entity notifies the United States Secret Service and the Federal Bureau of Investigation, in writing, of—

(A) the results of the risk assessment; and

(B) its decision to invoke the risk assessment exemption; and

(3) the United States Secret Service or the Federal Bureau of Investigation does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 311

1 if the business entity utilizes or participates in a se-  
 2 curity program that—

3 (A) is designed to block the use of the sen-  
 4 sitive personally identifiable information to ini-  
 5 tiate unauthorized financial transactions before  
 6 they are charged to the account of the indi-  
 7 vidual; and

8 (B) provides for notice to affected individ-  
 9 uals after a security breach that has resulted in  
 10 fraud or unauthorized transactions.

11 (2) LIMITATION.—The exemption by this sub-  
 12 section does not apply if—

13 (A) the information subject to the security  
 14 breach includes sensitive personally identifiable  
 15 information, other than a credit card or credit  
 16 card security code, of any type of the sensitive  
 17 personally identifiable information identified in  
 18 section 3; or

19 (B) the security breach includes both the  
 20 individual's credit card number and the individ-  
 21 ual's first and last name.

22 **SEC. 313. METHODS OF NOTICE.**

23 An agency or business entity shall be in compliance  
 24 with section 311 if it provides both:

1           ~~(1) INDIVIDUAL NOTICE.—~~Notice to individuals  
 2           by ~~1~~ of the following means:

3                   ~~(A) Written notification to the last known~~  
 4                   home mailing address of the individual in the  
 5                   records of the agency or business entity.

6                   ~~(B) Telephone notice to the individual per-~~  
 7                   sonally.

8                   ~~(C) E-mail notice, if the individual has~~  
 9                   consented to receive such notice and the notice  
 10                  is consistent with the provisions permitting elec-  
 11                  tronic transmission of notices under section 101  
 12                  of the Electronic Signatures in Global and Na-  
 13                  tional Commerce Act (~~15 U.S.C. 7001~~).

14           ~~(2) MEDIA NOTICE.—~~Notice to major media  
 15           outlets serving a State or jurisdiction, if the number  
 16           of residents of such State whose sensitive personally  
 17           identifiable information was, or is reasonably be-  
 18           lieved to have been, accessed or acquired by an un-  
 19           authorized person exceeds 5,000.

20   **SEC. 314. CONTENT OF NOTIFICATION.**

21           ~~(a) IN GENERAL.—~~Regardless of the method by  
 22           which notice is provided to individuals under section ~~313~~,  
 23           such notice shall include, to the extent possible—

24                   ~~(1)~~ a description of the categories of sensitive  
 25                   personally identifiable information that was, or is

1 reasonably believed to have been, accessed or ac-  
 2 quired by an unauthorized person;

3 ~~(2) a toll-free number—~~

4 ~~(A) that the individual may use to contact~~  
 5 ~~the agency or business entity, or the agent of~~  
 6 ~~the agency or business entity; and~~

7 ~~(B) from which the individual may learn~~  
 8 ~~what types of sensitive personally identifiable~~  
 9 ~~information the agency or business entity main-~~  
 10 ~~tained about that individual; and~~

11 ~~(3) the toll-free contact telephone numbers and~~  
 12 ~~addresses for the major credit reporting agencies.~~

13 ~~(b) ADDITIONAL CONTENT.—Notwithstanding sec-~~  
 14 ~~tion 319, a State may require that a notice under sub-~~  
 15 ~~section (a) shall also include information regarding victim~~  
 16 ~~protection assistance provided for by that State.~~

17 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**  
 18 **REPORTING AGENCIES.**

19 If an agency or business entity is required to provide  
 20 notification to more than 5,000 individuals under section  
 21 311(a), the agency or business entity shall also notify all  
 22 consumer reporting agencies that compile and maintain  
 23 files on consumers on a nationwide basis (as defined in  
 24 section 603(p) of the Fair Credit Reporting Act (15  
 25 U.S.C. 1681a(p)) of the timing and distribution of the no-

1 tices. Such notice shall be given to the consumer credit  
 2 reporting agencies without unreasonable delay and, if it  
 3 will not delay notice to the affected individuals, prior to  
 4 the distribution of notices to the affected individuals.

5 **SEC. 316. NOTICE TO LAW ENFORCEMENT.**

6 (a) ~~SECRET SERVICE AND FBI.~~—Any business entity  
 7 or agency shall notify the United States Secret Service  
 8 and the Federal Bureau of Investigation of the fact that  
 9 a security breach has occurred if—

10 (1) the number of individuals whose sensitive  
 11 personally identifying information was, or is reason-  
 12 ably believed to have been accessed or acquired by  
 13 an unauthorized person exceeds 10,000;

14 (2) the security breach involves a database,  
 15 networked or integrated databases, or other data  
 16 system containing the sensitive personally identifi-  
 17 able information of more than 1,000,000 individuals  
 18 nationwide;

19 (3) the security breach involves databases  
 20 owned by the Federal Government; or

21 (4) the security breach involves primarily sen-  
 22 sitive personally identifiable information of individ-  
 23 uals known to the agency or business entity to be  
 24 employees and contractors of the Federal Govern-

1       ment involved in national security or law enforce-  
2       ment.

3       (b) ~~FTC REVIEW OF THRESHOLDS.~~—The Federal  
4 Trade Commission may review and adjust the thresholds  
5 for notice to law enforcement under subsection (a), after  
6 notice and the opportunity for public comment, in a man-  
7 ner consistent with this section.

8       (c) ~~ADVANCE NOTICE TO LAW ENFORCEMENT.~~—Not  
9 later than 48 hours before notifying an individual of a se-  
10 curity breach under section 311, a business entity or agen-  
11 cy that is required to provide notice under this section  
12 shall notify the United States Secret Service and the Fed-  
13 eral Bureau of Investigation of the fact that the business  
14 entity or agency intends to provide the notice.

15       (d) ~~NOTICE TO OTHER LAW ENFORCEMENT AGEN-~~  
16 ~~CIES.~~—The United States Secret Service and the Federal  
17 Bureau of Investigation shall be responsible for noti-  
18 fying—

19               (1) the United States Postal Inspection Service;  
20       if the security breach involves mail fraud;

21               (2) the attorney general of each State affected  
22       by the security breach; and

23               (3) the Federal Trade Commission, if the secu-  
24       rity breach involves consumer reporting agencies

1 subject to the Fair Credit Reporting Act (15 U.S.C.  
2 1681 et seq.); or anticompetitive conduct.

3 (c) ~~TIMING OF NOTICES.~~—The notices required  
4 under this section shall be delivered as follows:

5 (1) Notice under subsection (a) shall be deliv-  
6 ered as promptly as possible, but not later than 14  
7 days after discovery of the events requiring notice.

8 (2) Notice under subsection (d) shall be deliv-  
9 ered not later than 14 days after the Service receives  
10 notice of a security breach from an agency or busi-  
11 ness entity.

12 **SEC. 317. ENFORCEMENT.**

13 (a) ~~CIVIL ACTIONS BY THE ATTORNEY GENERAL.~~—  
14 The Attorney General may bring a civil action in the ap-  
15 propriate United States district court against any business  
16 entity that engages in conduct constituting a violation of  
17 this subtitle and, upon proof of such conduct by a prepon-  
18 derance of the evidence, such business entity shall be sub-  
19 ject to a civil penalty of not more than \$1,000 per day  
20 per individual whose sensitive personally identifiable infor-  
21 mation was, or is reasonably believed to have been,  
22 accessed or acquired by an unauthorized person, up to a  
23 maximum of \$1,000,000 per violation, unless such conduct  
24 is found to be willful or intentional. In determining the  
25 amount of a civil penalty under this subsection, the court

1 shall take into account the degree of culpability of the  
 2 business entity; any prior violations of this subtitle by the  
 3 business entity; the ability of the business entity to pay;  
 4 the effect on the ability of the business entity to continue  
 5 to do business; and such other matters as justice may re-  
 6 quire.

7 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
 8 ERAL.—

9 (1) IN GENERAL.—If it appears that a business  
 10 entity has engaged, or is engaged, in any act or  
 11 practice constituting a violation of this subtitle, the  
 12 Attorney General may petition an appropriate dis-  
 13 trict court of the United States for an order—

14 (A) enjoining such act or practice; or

15 (B) enforcing compliance with this subtitle.

16 (2) ISSUANCE OF ORDER.—A court may issue  
 17 an order under paragraph (1), if the court finds that  
 18 the conduct in question constitutes a violation of this  
 19 subtitle.

20 (c) OTHER RIGHTS AND REMEDIES.—The rights and  
 21 remedies available under this subtitle are cumulative and  
 22 shall not affect any other rights and remedies available  
 23 under law.

24 (d) FRAUD ALERT.—Section 605A(b)(1) of the Fair  
 25 Credit Reporting Act (15 U.S.C. 1681e-1(b)(1)) is



1 amended by inserting “, or evidence that the consumer  
 2 has received notice that the consumer’s financial informa-  
 3 tion has or may have been compromised,” after “identity  
 4 theft report”.

5 **SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

6 (a) IN GENERAL.—

7 (1) CIVIL ACTIONS.—In any case in which the  
 8 attorney general of a State or any State or local law  
 9 enforcement agency authorized by the State attorney  
 10 general or by State statute to prosecute violations of  
 11 consumer protection law, has reason to believe that  
 12 an interest of the residents of that State has been  
 13 or is threatened or adversely affected by the engage-  
 14 ment of a business entity in a practice that is pro-  
 15 hibited under this subtitle, the State or the State or  
 16 local law enforcement agency on behalf of the resi-  
 17 dents of the agency’s jurisdiction, may bring a civil  
 18 action on behalf of the residents of the State or ju-  
 19 risdiction in a district court of the United States of  
 20 appropriate jurisdiction or any other court of com-  
 21 petent jurisdiction, including a State court, to—

22 (A) enjoin that practice;

23 (B) enforce compliance with this subtitle;

24 or

(C) civil penalties of not more than \$1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of \$1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general

1 of a State shall provide notice and a copy  
 2 of the complaint to the Attorney General  
 3 at the time the State attorney general files  
 4 the action.

5 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
 6 under subsection (a)(2), the Attorney General shall have  
 7 the right to—

8 (1) move to stay the action, pending the final  
 9 disposition of a pending Federal proceeding or ac-  
 10 tion;

11 (2) initiate an action in the appropriate United  
 12 States district court under section 317 and move to  
 13 consolidate all pending actions, including State ac-  
 14 tions, in such court;

15 (3) intervene in an action brought under sub-  
 16 section (a)(2); and

17 (4) file petitions for appeal.

18 (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
 19 eral has instituted a proceeding or action for a violation  
 20 of this subtitle or any regulations thereunder, no attorney  
 21 general of a State may, during the pendency of such pro-  
 22 ceeding or action, bring an action under this subtitle  
 23 against any defendant named in such criminal proceeding  
 24 or civil action for any violation that is alleged in that pro-  
 25 ceeding or action.

1       (d) CONSTRUCTION.—For purposes of bringing any  
 2 civil action under subsection (a), nothing in this subtitle  
 3 regarding notification shall be construed to prevent an at-  
 4 torney general of a State from exercising the powers con-  
 5 ferred on such attorney general by the laws of that State  
 6 to—

7           (1) conduct investigations;  
 8           (2) administer oaths or affirmations; or  
 9           (3) compel the attendance of witnesses or the  
 10 production of documentary and other evidence.

11       (e) VENUE; SERVICE OF PROCESS.—

12           (1) VENUE.—Any action brought under sub-  
 13 section (a) may be brought in—

14           (A) the district court of the United States  
 15 that meets applicable requirements relating to  
 16 venue under section 1391 of title 28, United  
 17 States Code; or

18           (B) another court of competent jurisdic-  
 19 tion.

20           (2) SERVICE OF PROCESS.—In an action  
 21 brought under subsection (a), process may be served  
 22 in any district in which the defendant—

23           (A) is an inhabitant; or

24           (B) may be found.

1       (f) NO PRIVATE CAUSE OF ACTION.—Nothing in this  
 2 subtitle establishes a private cause of action against a  
 3 business entity for violation of any provision of this sub-  
 4 title.

5 **SEC. 319. EFFECT ON FEDERAL AND STATE LAW.**

6       The provisions of this subtitle shall supersede any  
 7 other provision of Federal law or any provision of law of  
 8 any State relating to notification by a business entity en-  
 9 gaged in interstate commerce or an agency of a security  
 10 breach, except as provided in section 314(b).

11 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

12       There are authorized to be appropriated such sums  
 13 as may be necessary to cover the costs incurred by the  
 14 United States Secret Service to carry out investigations  
 15 and risk assessments of security breaches as required  
 16 under this subtitle.

17 **SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

18       The United States Secret Service and the Federal  
 19 Bureau of Investigation shall report to Congress not later  
 20 than 18 months after the date of enactment of this Act,  
 21 and upon the request by Congress thereafter, on—

22           (1) the number and nature of the security  
 23 breaches described in the notices filed by those busi-  
 24 ness entities invoking the risk assessment exemption  
 25 under section 312(b) and the response of the United

1 States Secret Service and the Federal Bureau of In-  
 2 vestigation to such notices; and

3 ~~(2) the number and nature of security breaches~~  
 4 ~~subject to the national security and law enforcement~~  
 5 ~~exemptions under section 312(a), provided that such~~  
 6 ~~report may not disclose the contents of any risk as-~~  
 7 ~~essment provided to the United States Secret Serv-~~  
 8 ~~ice and the Federal Bureau of Investigation pursu-~~  
 9 ~~ant to this subtitle.~~

10 **SEC. 322. EFFECTIVE DATE.**

11 This subtitle shall take effect on the expiration of the  
 12 date which is 90 days after the date of enactment of this  
 13 Act.

14 **TITLE IV—GOVERNMENT AC-**  
 15 **CESS TO AND USE OF COM-**  
 16 **MERCIAL DATA**

17 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**  
 18 **OF CONTRACTS.**

19 (a) **IN GENERAL.**—In considering contract awards  
 20 totaling more than \$500,000 and entered into after the  
 21 date of enactment of this Act with data brokers, the Ad-  
 22 ministrator of the General Services Administration shall  
 23 evaluate—

24 ~~(1) the data privacy and security program of a~~  
 25 ~~data broker to ensure the privacy and security of~~

1 data containing personally identifiable information;  
2 including whether such program adequately address-  
3 es privacy and security threats created by malicious  
4 software or code; or the use of peer-to-peer file shar-  
5 ing software;

6 (2) the compliance of a data broker with such  
7 program;

8 (3) the extent to which the databases and sys-  
9 tems containing personally identifiable information  
10 of a data broker have been compromised by security  
11 breaches; and

12 (4) the response by a data broker to such  
13 breaches, including the efforts by such data broker  
14 to mitigate the impact of such security breaches.

15 (b) COMPLIANCE SAFE HARBOR.—The data privacy  
16 and security program of a data broker shall be deemed  
17 sufficient for the purposes of subsection (a), if the data  
18 broker complies with or provides protection equal to indus-  
19 try standards, as identified by the Federal Trade Commis-  
20 sion, that are applicable to the type of personally identifi-  
21 able information involved in the ordinary course of busi-  
22 ness of such data broker.

23 (c) PENALTIES.—In awarding contracts with data  
24 brokers for products or services related to access, use,  
25 compilation, distribution, processing, analyzing, or evalu-

1 ating personally identifiable information, the Adminis-  
2 trator of the General Services Administration shall—

3       ~~(1) include monetary or other penalties—~~

4               ~~(A) for failure to comply with subtitles A~~  
5               ~~and B of title III; or~~

6               ~~(B) if a contractor knows or has reason to~~  
7               ~~know that the personally identifiable informa-~~  
8               ~~tion being provided is inaccurate, and provides~~  
9               ~~such inaccurate information; and~~

10       ~~(2) require a data broker that engages service~~  
11       ~~providers not subject to subtitle A of title III for re-~~  
12       ~~sponsibilities related to sensitive personally identifi-~~  
13       ~~able information to—~~

14               ~~(A) exercise appropriate due diligence in~~  
15               ~~selecting those service providers for responsibil-~~  
16               ~~ities related to personally identifiable informa-~~  
17               ~~tion;~~

18               ~~(B) take reasonable steps to select and re-~~  
19               ~~tain service providers that are capable of main-~~  
20               ~~taining appropriate safeguards for the security,~~  
21               ~~privacy, and integrity of the personally identifi-~~  
22               ~~able information at issue; and~~

23               ~~(C) require such service providers, by con-~~  
24               ~~tract, to implement and maintain appropriate~~



1 measures designed to meet the objectives and  
 2 requirements in title III.

3 ~~(d) LIMITATION.—The penalties under subsection (e)~~  
 4 ~~shall not apply to a data broker providing information that~~  
 5 ~~is accurately and completely recorded from a public record~~  
 6 ~~source or licensor.~~

7 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECU-**  
 8 **RITY PRACTICES OF CONTRACTORS AND**  
 9 **THIRD PARTY BUSINESS ENTITIES.**

10 Section 3544(b) of title 44, United States Code, is  
 11 amended—

12 (1) in paragraph (7)(C)(iii), by striking “and”  
 13 after the semicolon;

14 (2) in paragraph (8), by striking the period and  
 15 inserting “; and”; and

16 (3) by adding at the end the following:

17 “(9) procedures for evaluating and auditing the  
 18 information security practices of contractors or third  
 19 party business entities supporting the information  
 20 systems or operations of the agency involving per-  
 21 sonally identifiable information (as that term is de-  
 22 fined in section 3 of the Personal Data Privacy and  
 23 Security Act of 2011) and ensuring remedial action  
 24 to address any significant deficiencies.”.

1 **SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**  
 2 **USE OF COMMERCIAL INFORMATION SERV-**  
 3 **ICES CONTAINING PERSONALLY IDENTIFI-**  
 4 **ABLE INFORMATION.**

5 (a) ~~IN GENERAL.~~—Section 208(b)(1) of the ~~E-Gov-~~  
 6 ~~ernment Act of 2002 (44 U.S.C. 3501 note)~~ is amended—

7 (1) in subparagraph (A)(i), by striking “or”;  
 8 and

9 (2) in subparagraph (A)(ii), by striking the pe-  
 10 riod and inserting “; or”; and

11 (3) by inserting after clause (ii) the following:

12 “(iii) purchasing or subscribing for a  
 13 fee to personally identifiable information  
 14 from a data broker (as such terms are de-  
 15 fined in section 3 of the Personal Data  
 16 Privacy and Security Act of 2011).”.

17 (b) ~~LIMITATION.~~—Notwithstanding any other provi-  
 18 sion of law, commencing 1 year after the date of enact-  
 19 ment of this Act, no Federal agency may enter into a con-  
 20 tract with a data broker to access for a fee any database  
 21 consisting primarily of personally identifiable information  
 22 concerning United States persons (other than news report-  
 23 ing or telephone directories) unless the head of such de-  
 24 partment or agency—

25 (1) completes a privacy impact assessment  
 26 under section 208 of the ~~E-Government Act of 2002~~

1       ~~(44 U.S.C. 3501~~ note), which shall subject to the  
2       provision in that Act pertaining to sensitive informa-  
3       tion, include a description of—

4               ~~(A)~~ such database;

5               ~~(B)~~ the name of the data broker from  
6       whom it is obtained; and

7               ~~(C)~~ the amount of the contract for use;

8       ~~(2)~~ adopts regulations that specify—

9               ~~(A)~~ the personnel permitted to access, ana-  
10      lyze, or otherwise use such databases;

11              ~~(B)~~ standards governing the access, anal-  
12      ysis, or use of such databases;

13              ~~(C)~~ any standards used to ensure that the  
14      personally identifiable information accessed,  
15      analyzed, or used is the minimum necessary to  
16      accomplish the intended legitimate purpose of  
17      the Federal agency;

18              ~~(D)~~ standards limiting the retention and  
19      redisclosure of personally identifiable informa-  
20      tion obtained from such databases;

21              ~~(E)~~ procedures ensuring that such data  
22      meet standards of accuracy, relevance, com-  
23      pleteness, and timeliness;

1           (F) the auditing and security measures to  
 2           protect against unauthorized access, analysis,  
 3           use, or modification of data in such databases;

4           (G) applicable mechanisms by which indi-  
 5           viduals may secure timely redress for any ad-  
 6           verse consequences wrongly incurred due to the  
 7           access, analysis, or use of such databases;

8           (H) mechanisms, if any, for the enforce-  
 9           ment and independent oversight of existing or  
 10          planned procedures, policies, or guidelines; and

11          (I) an outline of enforcement mechanisms  
 12          for accountability to protect individuals and the  
 13          public against unlawful or illegitimate access or  
 14          use of databases; and

15          ~~(J)~~ incorporates into the contract or other  
 16          agreement totaling more than \$500,000, provi-  
 17          sions—

18                 (A) providing for penalties—

19                         (i) for failure to comply with title III  
 20                         of this Act; or

21                         (ii) if the entity knows or has reason  
 22                         to know that the personally identifiable in-  
 23                         formation being provided to the Federal  
 24                         department or agency is inaccurate, and  
 25                         provides such inaccurate information; and

1           ~~(B)~~ requiring a data broker that engages  
 2           service providers not subject to subtitle A of  
 3           title III for responsibilities related to sensitive  
 4           personally identifiable information to—

5                   (i) exercise appropriate due diligence  
 6                   in selecting those service providers for re-  
 7                   sponsibilities related to personally identifi-  
 8                   able information;

9                   (ii) take reasonable steps to select and  
 10                  retain service providers that are capable of  
 11                  maintaining appropriate safeguards for the  
 12                  security, privacy, and integrity of the per-  
 13                  sonally identifiable information at issue;  
 14                  and

15                  (iii) require such service providers, by  
 16                  contract, to implement and maintain ap-  
 17                  propriate measures designed to meet the  
 18                  objectives and requirements in title III.

19       ~~(c) LIMITATION ON PENALTIES.—~~The penalties  
 20       under subsection ~~(b)(3)(A)~~ shall not apply to a data  
 21       broker providing information that is accurately and com-  
 22       pletely recorded from a public record source.

23       ~~(d) STUDY OF GOVERNMENT USE.—~~

24               ~~(1) SCOPE OF STUDY.—~~Not later than 180  
 25       days after the date of enactment of this Act, the

1 Comptroller General of the United States shall con-  
 2 duct a study and audit and prepare a report on Fed-  
 3 eral agency actions to address the recommendations  
 4 in the Government Accountability Office's April  
 5 2006 report on agency adherence to key privacy  
 6 principles in using data brokers or commercial data-  
 7 bases containing personally identifiable information.

8 (2) REPORT.—A copy of the report required  
 9 under paragraph (1) shall be submitted to Congress.

## 10 **TITLE V—COMPLIANCE WITH** 11 **STATUTORY PAY-AS-YOU-GO ACT**

### 12 **SEC. 501. BUDGET COMPLIANCE.**

13 The budgetary effects of this Act, for the purpose of  
 14 complying with the Statutory Pay-As-You-Go Act of 2010,  
 15 shall be determined by reference to the latest statement  
 16 titled “Budgetary Effects of PAYGO Legislation” for this  
 17 Act, submitted for printing in the Congressional Record  
 18 by the Chairman of the Senate Budget Committee, pro-  
 19 vided that such statement has been submitted prior to the  
 20 vote on passage.

### 21 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

22 (a) *SHORT TITLE.*—This Act may be cited as the “Per-  
 23 sonal Data Privacy and Security Act of 2011”.

24 (b) *TABLE OF CONTENTS.*—The table of contents of this  
 25 Act is as follows:

*Sec. 1. Short title; table of contents.*

- Sec. 2. Findings.*  
*Sec. 3. Definitions.*

**TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND  
OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY**

- Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.*  
*Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.*  
*Sec. 103. Penalties for fraud and related activity in connection with computers.*  
*Sec. 104. Trafficking in passwords.*  
*Sec. 105. Conspiracy and attempted computer fraud offenses.*  
*Sec. 106. Criminal and civil forfeiture for fraud and related activity in connection with computers.*  
*Sec. 107. Limitation on civil actions involving unauthorized use.*  
*Sec. 108. Reporting of certain criminal cases.*  
*Sec. 109. Damage to critical infrastructure computers.*  
*Sec. 110. Limitation on actions involving unauthorized use.*

**TITLE II—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE  
INFORMATION**

*Subtitle A—A Data Privacy and Security Program*

- Sec. 201. Purpose and applicability of data privacy and security program.*  
*Sec. 202. Requirements for a personal data privacy and security program.*  
*Sec. 203. Enforcement.*  
*Sec. 204. Relation to other laws.*

*Subtitle B—Security Breach Notification*

- Sec. 211. Notice to individuals.*  
*Sec. 212. Exemptions.*  
*Sec. 213. Methods of notice.*  
*Sec. 214. Content of notification.*  
*Sec. 215. Coordination of notification with credit reporting agencies.*  
*Sec. 216. Notice to law enforcement.*  
*Sec. 217. Enforcement.*  
*Sec. 218. Enforcement by State attorneys general.*  
*Sec. 219. Effect on Federal and State law.*  
*Sec. 220. Reporting on exemptions.*  
*Sec. 221. Effective date.*

**TITLE III—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT**

- Sec. 301. Budget compliance.*

**1 SEC. 2. FINDINGS.**

2 Congress finds that—

- 3 (1) databases of personally identifiable informa-  
 4 tion are increasingly prime targets of hackers, iden-

1        *tity thieves, rogue employees, and other criminals, in-*  
2        *cluding organized and sophisticated criminal oper-*  
3        *ations;*

4            *(2) identity theft is a serious threat to the Na-*  
5        *tion's economic stability, national security, homeland*  
6        *security, cybersecurity, the development of e-com-*  
7        *merce, and the privacy rights of Americans;*

8            *(3) security breaches are a serious threat to con-*  
9        *sumer confidence, homeland security, national secu-*  
10       *rity, e-commerce, and economic stability;*

11           *(4) it is important for business entities that own,*  
12       *use, or license personally identifiable information to*  
13       *adopt reasonable procedures to ensure the security,*  
14       *privacy, and confidentiality of that personally identi-*  
15       *fiable information;*

16           *(5) individuals whose personal information has*  
17       *been compromised or who have been victims of iden-*  
18       *tity theft should receive the necessary information and*  
19       *assistance to mitigate their damages and to restore*  
20       *the integrity of their personal information and identi-*  
21       *ties;*

22           *(6) data misuse and use of inaccurate data have*  
23       *the potential to cause serious or irreparable harm to*  
24       *an individual's livelihood, privacy, and liberty and*



1       undermine efficient and effective business and govern-  
 2       ment operations;

3               (7) government access to commercial data can  
 4       potentially improve safety, law enforcement, and na-  
 5       tional security; and

6               (8) because government use of commercial data  
 7       containing personal information potentially affects  
 8       individual privacy, and law enforcement and na-  
 9       tional security operations, there is a need for Con-  
 10      gress to exercise oversight over government use of com-  
 11      mercial data.

12   **SEC. 3. DEFINITIONS.**

13       *In this Act, the following definitions shall apply:*

14               (1) *AFFILIATE.*—The term “affiliate” means per-  
 15      sons related by common ownership or by corporate  
 16      control.

17               (2) *AGENCY.*—The term “agency” has the same  
 18      meaning given such term in section 551 of title 5,  
 19      United States Code.

20               (3) *BUSINESS ENTITY.*—The term “business enti-  
 21      ty” means any organization, corporation, trust, part-  
 22      nership, sole proprietorship, unincorporated associa-  
 23      tion, or venture established to make a profit, or non-  
 24      profit.

1           (4) *DATA SYSTEM COMMUNICATION INFORMATION.*—*The term “data system communication information” means dialing, routing, addressing, or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.*

8           (5) *DESIGNATED ENTITY.*—*The term “designated entity” means the Federal Government entity designated by the Secretary of Homeland Security under section 216(a).*

12           (6) *ENCRYPTION.*—*The term “encryption”—*  
 13                 *(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been generally accepted by experts in the field of information security that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and*

20                 *(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.*

23           (7) *IDENTITY THEFT.*—*The term “identity theft” means a violation of section 1028(a)(7) of title 18, United States Code.*

1           (8) *PERSONALLY IDENTIFIABLE INFORMATION*.—

2           *The term “personally identifiable information” means*  
 3           *any information, or compilation of information, in*  
 4           *electronic or digital form that is a means of identi-*  
 5           *fication, as defined by section 1028(d)(7) of title 18,*  
 6           *United State Code.*

7           (9) *PUBLIC RECORD SOURCE*.—*The term “public*  
 8           *record source” means the Congress, any agency, any*  
 9           *State or local government agency, the government of*  
 10           *the District of Columbia and governments of the terri-*  
 11           *tories or possessions of the United States, and Fed-*  
 12           *eral, State or local courts, courts martial and mili-*  
 13           *tary commissions, that maintain personally identifi-*  
 14           *able information in records available to the public.*

15           (10) *SECURITY BREACH*.—

16           (A) *IN GENERAL*.—*The term “security*  
 17           *breach” means compromise of the security, con-*  
 18           *fidentiality, or integrity of, or the loss of, com-*  
 19           *puterized data that result in, or that there is a*  
 20           *reasonable basis to conclude has resulted in—*

21                     (i) *the unauthorized acquisition of sen-*  
 22                     *sitive personally identifiable information;*  
 23                     *and*

24                     (ii) *access to sensitive personally iden-*  
 25                     *tifiable information that is for an unau-*

1            *thorized purpose, or in excess of authoriza-*  
 2            *tion.*

3            (B) *EXCLUSION.—The term “security*  
 4            *breach” does not include—*

5                    (i) *a good faith acquisition of sensitive*  
 6                    *personally identifiable information by a*  
 7                    *business entity or agency, or an employee or*  
 8                    *agent of a business entity or agency, if the*  
 9                    *sensitive personally identifiable information*  
 10                   *is not subject to further unauthorized disclo-*  
 11                   *sure;*

12                   (ii) *the release of a public record not*  
 13                   *otherwise subject to confidentiality or non-*  
 14                   *disclosure requirements or the release of in-*  
 15                   *formation obtained from a public record,*  
 16                   *including information obtained from a news*  
 17                   *report or periodical; or*

18                   (iii) *any lawfully authorized investiga-*  
 19                   *tive, protective, or intelligence activity of a*  
 20                   *law enforcement or intelligence agency of*  
 21                   *the United States, a State, or a political*  
 22                   *subdivision of a State.*

23            (11) *SENSITIVE PERSONALLY IDENTIFIABLE IN-*  
 24            *FORMATION.—The term “sensitive personally identifi-*  
 25            *able information” means any information or com-*

1        *pilation of information, in electronic or digital form*  
2        *that includes the following:*

3                *(A) An individual's first and last name or*  
4                *first initial and last name in combination with*  
5                *any two of the following data elements:*

6                        *(i) Home address or telephone number.*

7                        *(ii) Mother's maiden name.*

8                        *(iii) Month, day, and year of birth.*

9                *(B) A non-truncated social security number,*  
10                *driver's license number, passport number, or*  
11                *alien registration number or other government-*  
12                *issued unique identification number.*

13                *(C) Unique biometric data such as a finger*  
14                *print, voice print, a retina or iris image, or any*  
15                *other unique physical representation.*

16                *(D) A unique account identifier, including*  
17                *a financial account number or credit or debit*  
18                *card number, electronic identification number,*  
19                *user name, or routing code.*

20                *(E) Any combination of the following data*  
21                *elements:*

22                        *(i) An individual's first and last name*  
23                        *or first initial and last name.*

24                        *(ii) A unique account identifier, in-*  
25                        *cluding a financial account number or cred-*

1           it or debit card number, electronic identi-  
 2           fication number, user name, or routing  
 3           code.

4           (iii) Any security code, access code, or  
 5           password, or source code that could be used  
 6           to generate such codes or passwords.

7           (12) *SERVICE PROVIDER.*—The term “service  
 8           provider” means a business entity that provides elec-  
 9           tronic data transmission, routing, intermediate and  
 10          transient storage, or connections to its system or net-  
 11          work, where the business entity providing such serv-  
 12          ices does not select or modify the content of the elec-  
 13          tronic data, is not the sender or the intended recipi-  
 14          ent of the data, and the business entity transmits,  
 15          routes, stores, or provides connections for personal in-  
 16          formation in a manner that personal information is  
 17          undifferentiated from other types of data that such  
 18          business entity transmits, routes, stores, or provides  
 19          connections. Any such business entity shall be treated  
 20          as a service provider under this Act only to the extent  
 21          that it is engaged in the provision of such trans-  
 22          mission, routing, intermediate and transient storage  
 23          or connections.

1 ***TITLE I—ENHANCING PUNISH-***  
 2 ***MENT FOR IDENTITY THEFT***  
 3 ***AND OTHER VIOLATIONS OF***  
 4 ***DATA PRIVACY AND SECURITY***

5 ***SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION***  
 6 ***WITH UNAUTHORIZED ACCESS TO PERSON-***  
 7 ***ALLY IDENTIFIABLE INFORMATION.***

8 *Section 1961(1) of title 18, United States Code, is*  
 9 *amended by inserting “section 1030 (relating to fraud and*  
 10 *related activity in connection with computers) if the act*  
 11 *is a felony,” before “section 1084”.*

12 ***SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-***  
 13 ***ING SENSITIVE PERSONALLY IDENTIFIABLE***  
 14 ***INFORMATION.***

15 *(a) IN GENERAL.—Chapter 47 of title 18, United*  
 16 *States Code, is amended by adding at the end the following:*

17 ***“§1041. Concealment of security breaches involving***  
 18 ***sensitive personally identifiable informa-***  
 19 ***tion***

20 *“(a) IN GENERAL.—Whoever, having knowledge of a*  
 21 *security breach and of the fact that notice of such security*  
 22 *breach is required under title II of the Personal Data Pri-*  
 23 *vacy and Security Act of 2011, intentionally and willfully*  
 24 *conceals the fact of such security breach, shall, in the event*  
 25 *that such security breach results in economic harm to any*

1 *individual in the amount of \$1,000 or more, be fined under*  
 2 *this title or imprisoned for not more than 5 years, or both.*

3 “(b) *PERSON DEFINED.*—*For purposes of subsection*  
 4 *(a), the term ‘person’ has the same meaning as in section*  
 5 *1030(e)(12) of title 18, United States Code.*

6 “(c) *NOTICE REQUIREMENT.*—*Any person seeking an*  
 7 *exemption under section 212(b) of the Personal Data Pri-*  
 8 *vacy and Security Act of 2011 shall be immune from pros-*  
 9 *ecution under this section if the Federal Trade Commission*  
 10 *does not indicate, in writing, that such notice be given*  
 11 *under section 212(b)(3) of such Act.”.*

12 (b) *CONFORMING AND TECHNICAL AMENDMENTS.*—  
 13 *The table of sections for chapter 47 of title 18, United States*  
 14 *Code, is amended by adding at the end the following:*

*“1041. Concealment of security breaches involving sensitive personally identifiable information.”.*

15 (c) *ENFORCEMENT AUTHORITY.*—

16 (1) *IN GENERAL.*—*The United States Secret*  
 17 *Service and Federal Bureau of Investigation shall*  
 18 *have the authority to investigate offenses under this*  
 19 *section.*

20 (2) *NONEXCLUSIVITY.*—*The authority granted in*  
 21 *paragraph (1) shall not be exclusive of any existing*  
 22 *authority held by any other Federal agency.*



1 **SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY**  
2 **IN CONNECTION WITH COMPUTERS.**

3 *Section 1030(c) of title 18, United States Code, is*  
4 *amended to read as follows:*

5 “(c) *The punishment for an offense under subsection*  
6 *(a) or (b) of this section is—*

7 “(1) *a fine under this title or imprisonment for*  
8 *not more than 20 years, or both, in the case of an of-*  
9 *fense under subsection (a)(1) of this section;*

10 “(2)(A) *except as provided in subparagraph (B),*  
11 *a fine under this title or imprisonment for not more*  
12 *than 3 years, or both, in the case of an offense under*  
13 *subsection (a)(2); or*

14 “(B) *a fine under this title or imprisonment for*  
15 *not more than ten years, or both, in the case of an*  
16 *offense under paragraph (a)(2) of this section, if—*

17 “(i) *the offense was committed for purposes*  
18 *of commercial advantage or private financial*  
19 *gain;*

20 “(ii) *the offense was committed in the fur-*  
21 *therance of any criminal or tortious act in viola-*  
22 *tion of the Constitution or laws of the United*  
23 *States, or of any State; or*

24 “(iii) *the value of the information obtained,*  
25 *or that would have been obtained if the offense*  
26 *was completed, exceeds \$5,000;*

1           “(3) a fine under this title or imprisonment for  
2           not more than 1 year, or both, in the case of an of-  
3           fense under subsection (a)(3) of this section;

4           “(4) a fine under this title or imprisonment of  
5           not more than 20 years, or both, in the case of an of-  
6           fense under subsection (a)(4) of this section;

7           “(5)(A) except as provided in subparagraph (D),  
8           a fine under this title, imprisonment for not more  
9           than 20 years, or both, in the case of an offense under  
10          subsection (a)(5)(A) of this section, if the offense  
11          caused—

12               “(i) loss to 1 or more persons during any  
13               1-year period (and, for purposes of an investiga-  
14               tion, prosecution, or other proceeding brought by  
15               the United States only, loss resulting from a re-  
16               lated course of conduct affecting 1 or more other  
17               protected computers) aggregating at least \$5,000  
18               in value;

19               “(ii) the modification or impairment, or  
20               potential modification or impairment, of the  
21               medical examination, diagnosis, treatment, or  
22               care of 1 or more individuals;

23               “(iii) physical injury to any person;

24               “(iv) a threat to public health or safety;

1           “(v) damage affecting a computer used by,  
2           or on behalf of, an entity of the United States  
3           Government in furtherance of the administration  
4           of justice, national defense, or national security;  
5           or

6           “(vi) damage affecting 10 or more protected  
7           computers during any 1-year period;

8           “(B) a fine under this title, imprisonment for  
9           not more than 10 years, or both, in the case of an of-  
10          fense under subsection (a)(5)(B), if the offense caused  
11          a harm provided in clause (i) through (vi) of sub-  
12          paragraph (A) of this subsection;

13          “(C) if the offender attempts to cause or know-  
14          ingly or recklessly causes death from conduct in viola-  
15          tion of subsection (a)(5)(A), a fine under this title,  
16          imprisonment for any term of years or for life, or  
17          both; or

18          “(D) a fine under this title, imprisonment for  
19          not more than 1 year, or both, for any other offense  
20          under subsection (a)(5);

21          “(6) a fine under this title or imprisonment for  
22          not more than 10 years, or both, in the case of an of-  
23          fense under subsection (a)(6) of this section; or

1           “(7) a fine under this title or imprisonment for  
 2           not more than 10 years, or both, in the case of an of-  
 3           fense under subsection (a)(7) of this section.”.

4   **SEC. 104. TRAFFICKING IN PASSWORDS.**

5           Section 1030(a) of title 18, United States Code, is  
 6           amended by striking paragraph (6) and inserting the fol-  
 7           lowing:

8           “(6) knowingly and with intent to defraud traf-  
 9           fics (as defined in section 1029) in—

10           “(A) any password or similar information  
 11           through which a protected computer as defined  
 12           in subparagraphs (A) and (B) of subsection  
 13           (e)(2) may be accessed without authorization; or

14           “(B) any means of access through which a  
 15           protected computer as defined in subsection  
 16           (e)(2)(A) may be accessed without authoriza-  
 17           tion.”.

18   **SEC. 105. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD**

19           **OFFENSES.**

20           Section 1030(b) of title 18, United States Code, is  
 21           amended by inserting “for the completed offense” after  
 22           “punished as provided”.

1 **SEC. 106. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD**  
 2 **AND RELATED ACTIVITY IN CONNECTION**  
 3 **WITH COMPUTERS.**

4 *Section 1030 of title 18, United States Code, is amend-*  
 5 *ed by striking subsections (i) and (j) and inserting the fol-*  
 6 *lowing:*

7 “(i) **CRIMINAL FORFEITURE.**—

8 “(1) *The court, in imposing sentence on any per-*  
 9 *son convicted of a violation of this section, or con-*  
 10 *victed of conspiracy to violate this section, shall order,*  
 11 *in addition to any other sentence imposed and irre-*  
 12 *spective of any provision of State law, that such per-*  
 13 *son forfeit to the United States—*

14 “(A) *such person’s interest in any property,*  
 15 *real or personal, that was used, or intended to*  
 16 *be used, to commit or facilitate the commission*  
 17 *of such violation; and*

18 “(B) *any property, real or personal, consti-*  
 19 *tuting or derived from any gross proceeds, or*  
 20 *any property traceable to such property, that*  
 21 *such person obtained, directly or indirectly, as a*  
 22 *result of such violation.*

23 “(2) *The criminal forfeiture of property under*  
 24 *this subsection, including any seizure and disposition*  
 25 *of the property, and any related judicial or adminis-*  
 26 *trative proceeding, shall be governed by the provisions*

1       *of section 413 of the Comprehensive Drug Abuse Pre-*  
 2       *vention and Control Act of 1970 (21 U.S.C. 853), ex-*  
 3       *cept subsection (d) of that section.*

4       “(j) *CIVIL FORFEITURE.*—

5               “(1) *The following shall be subject to forfeiture to*  
 6       *the United States and no property right, real or per-*  
 7       *sonal, shall exist in them:*

8                       “(A) *Any property, real or personal, that*  
 9               *was used, or intended to be used, to commit or*  
 10           *facilitate the commission of any violation of this*  
 11           *section, or a conspiracy to violate this section.*

12                      “(B) *Any property, real or personal, consti-*  
 13           *tuting or derived from any gross proceeds ob-*  
 14           *tained directly or indirectly, or any property*  
 15           *traceable to such property, as a result of the com-*  
 16           *mission of any violation of this section, or a con-*  
 17           *spiracy to violate this section.*

18               “(2) *Seizures and forfeitures under this sub-*  
 19       *section shall be governed by the provisions in chapter*  
 20       *46 of title 18, United States Code, relating to civil*  
 21       *forfeitures, except that such duties as are imposed on*  
 22       *the Secretary of the Treasury under the customs laws*  
 23       *described in section 981(d) of title 18, United States*  
 24       *Code, shall be performed by such officers, agents and*  
 25       *other persons as may be designated for that purpose*

1       *by the Secretary of Homeland Security or the Attor-*  
 2       *ney General.”.*

3   **SEC. 107. LIMITATION ON CIVIL ACTIONS INVOLVING UNAU-**  
 4       **THORIZED USE.**

5       *Section 1030(g) of title 18, United States Code, is*  
 6   *amended—*

7           *(1) by inserting “(1)” before “Any person”; and*  
 8           *(2) by adding at the end the following:*

9       *“(2) No action may be brought under this subsection*  
 10   *if a violation of a contractual obligation or agreement, such*  
 11   *as an acceptable use policy or terms of service agreement,*  
 12   *constitutes the sole basis for determining that access to the*  
 13   *protected computer is unauthorized, or in excess of author-*  
 14   *ization.”.*

15   **SEC. 108. REPORTING OF CERTAIN CRIMINAL CASES.**

16       *Section 1030 of title 18, United States Code, is amend-*  
 17   *ed by adding at the end the following:*

18       *“(k) REPORTING CERTAIN CRIMINAL CASES.—Not*  
 19   *later than 1 year after the date of the enactment of this*  
 20   *Act, and annually thereafter, the Attorney General shall re-*  
 21   *port to the Committee on the Judiciary of the Senate and*  
 22   *the Committee on the Judiciary of the House of Representa-*  
 23   *tives the number of criminal cases brought under subsection*  
 24   *(a) that involve conduct in which —*

25           *“(1) the defendant—*

1           “(A) exceeded authorized access to a non-  
2           governmental computer; or

3           “(B) accessed a non-governmental computer  
4           without authorization; and

5           “(2) the sole basis for the Government deter-  
6           mining that access to the non-governmental computer  
7           was unauthorized, or in excess of authorization was  
8           that the defendant violated a contractual obligation or  
9           agreement with a service provider or employer, such  
10          as an acceptable use policy or terms of service agree-  
11          ment.”.

12 **SEC. 109. DAMAGE TO CRITICAL INFRASTRUCTURE COM-**  
13 **PUTERS.**

14       (a) *IN GENERAL.*—Chapter 47 of title 18, United  
15 States Code, is amended by inserting after section 1030 the  
16 following:

17 **“§ 1030A. Aggravated damage to a critical infrastruc-**  
18 **ture computer**

19       “(a) *DEFINITIONS.*—In this section—

20           “(1) the terms ‘computer’ and ‘damage’ have the  
21 meanings given such terms in section 1030; and

22           “(2) the term ‘critical infrastructure computer’  
23 means a computer that manages or controls systems  
24 or assets vital to national defense, national security,  
25 national economic security, public health or safety, or



1       *any combination of those matters, whether publicly or*  
 2       *privately owned or operated, including—*

3               “(A) *gas and oil production, storage, and*  
 4       *delivery systems;*

5               “(B) *water supply systems;*

6               “(C) *telecommunication networks;*

7               “(D) *electrical power delivery systems;*

8               “(E) *finance and banking systems;*

9               “(F) *emergency services;*

10              “(G) *transportation systems and services;*

11              *and*

12              “(H) *government operations that provide*  
 13       *essential services to the public*

14       “(b) *OFFENSE.—It shall be unlawful to, during and*  
 15       *in relation to a felony violation of section 1030, inten-*  
 16       *tionally cause or attempt to cause damage to a critical in-*  
 17       *frastructure computer, and such damage results in (or, in*  
 18       *the case of an attempt, would, if completed have resulted*  
 19       *in) the substantial impairment—*

20              “(1) *of the operation of the critical infrastruc-*  
 21       *ture computer; or*

22              “(2) *of the critical infrastructure associated with*  
 23       *the computer.*

1       “(c) *PENALTY.*—Any person who violates subsection  
2 (b) shall be fined under this title, imprisoned for not less  
3 than 3 years nor more than 20 years, or both.

4       “(d) *CONSECUTIVE SENTENCE.*—Notwithstanding any  
5 other provision of law—

6               “(1) a court shall not place on probation any  
7 person convicted of a violation of this section;

8               “(2) except as provided in paragraph (4), no  
9 term of imprisonment imposed on a person under this  
10 section shall run concurrently with any other term of  
11 imprisonment, including any term of imprisonment  
12 imposed on the person under any other provision of  
13 law, including any term of imprisonment imposed for  
14 the felony violation section 1030;

15               “(3) in determining any term of imprisonment  
16 to be imposed for a felony violation of section 1030,  
17 a court shall not in any way reduce the term to be  
18 imposed for such crime so as to compensate for, or  
19 otherwise take into account, any separate term of im-  
20 prisonment imposed or to be imposed for a violation  
21 of this section; and

22               “(4) a term of imprisonment imposed on a per-  
23 son for a violation of this section may, in the discre-  
24 tion of the court, run concurrently, in whole or in  
25 part, only with another term of imprisonment that is

1        *imposed by the court at the same time on that person*  
 2        *for an additional violation of this section, provided*  
 3        *that such discretion shall be exercised in accordance*  
 4        *with any applicable guidelines and policy statements*  
 5        *issued by the United States Sentencing Commission*  
 6        *pursuant to section 994 of title 28.”.*

7        *(b) TECHNICAL AND CONFORMING AMENDMENT.—The*  
 8        *table of sections for chapter 47 of title 18, United States*  
 9        *Code, is amended by inserting after the item relating to*  
 10       *section 1030 the following:*

*“1030A. Aggravated damage to a critical infrastructure computer.”.*

11       **SEC. 110. LIMITATION ON ACTIONS INVOLVING UNAUTHOR-**  
 12       **IZED USE.**

13       *Section 1030(e)(6) of title 18, United States Code, is*  
 14       *amended by striking “alter;” and inserting “alter, but does*  
 15       *not include access in violation of a contractual obligation*  
 16       *or agreement, such as an acceptable use policy or terms of*  
 17       *service agreement, with an Internet service provider, Inter-*  
 18       *net website, or non-government employer, if such violation*  
 19       *constitutes the sole basis for determining that access to a*  
 20       *protected computer is unauthorized;”.*

1 ***TITLE II—PRIVACY AND SECU-***  
 2 ***RITY OF PERSONALLY IDENTI-***  
 3 ***FIABLE INFORMATION***

4 ***Subtitle A—A Data Privacy and***  
 5 ***Security Program***

6 ***SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY***  
 7 ***AND SECURITY PROGRAM.***

8 (a) *PURPOSE.*—*The purpose of this subtitle is to en-*  
 9 *sure standards for developing and implementing adminis-*  
 10 *trative, technical, and physical safeguards to protect the se-*  
 11 *curity of sensitive personally identifiable information.*

12 (b) *IN GENERAL.*—*A business entity engaging in*  
 13 *interstate commerce that involves collecting, accessing,*  
 14 *transmitting, using, storing, or disposing of sensitive per-*  
 15 *sonally identifiable information in electronic or digital*  
 16 *form on 10,000 or more United States persons is subject*  
 17 *to the requirements for a data privacy and security pro-*  
 18 *gram under section 202 for protecting sensitive personally*  
 19 *identifiable information.*

20 (c) *LIMITATIONS.*—*Notwithstanding any other obliga-*  
 21 *tion under this subtitle, this subtitle does not apply to the*  
 22 *following:*

23 (1) *FINANCIAL INSTITUTIONS.*—*Financial insti-*  
 24 *tutions—*

1           (A) *subject to the data security requirements*  
 2           *and standards under section 501(b) of the*  
 3           *Gramm-Leach-Bliley Act (15 U.S.C. 6801(b));*  
 4           *and*

5           (B) *subject to the jurisdiction of an agency*  
 6           *or authority described in section 505(a) of the*  
 7           *Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).*

8           (2) *HIPAA REGULATED ENTITIES.—*

9           (A) *COVERED ENTITIES.—Covered entities*  
 10           *subject to the Health Insurance Portability and*  
 11           *Accountability Act of 1996 (42 U.S.C. 1301 et*  
 12           *seq.), including the data security requirements*  
 13           *and implementing regulations of that Act.*

14           (B) *BUSINESS ENTITIES.—A Business enti-*  
 15           *ty shall be deemed in compliance with this Act*  
 16           *if the business entity—*

17                   (i) *is acting as a business associate, as*  
 18                   *that term is defined under the Health In-*  
 19                   *surance Portability and Accountability Act*  
 20                   *of 1996 (42 U.S.C. 1301 et seq.) and is in*  
 21                   *compliance with the requirements imposed*  
 22                   *under that Act and implementing regula-*  
 23                   *tions promulgated under that Act; and*

24                   (ii) *is subject to, and currently in com-*  
 25                   *pliance, with the privacy and data security*

1            *requirements under sections 13401 and*  
 2            *13404 of division A of the American Rein-*  
 3            *vestment and Recovery Act of 2009 (42*  
 4            *U.S.C. 17931 and 17934) and imple-*  
 5            *menting regulations promulgated under*  
 6            *such sections.*

7            (3) *SERVICE PROVIDERS.*—*A service provider for*  
 8            *any electronic communication by a third-party, to the*  
 9            *extent that the service provider is exclusively engaged*  
 10           *in the transmission, routing, or temporary, inter-*  
 11           *mediate, or transient storage of that communication.*

12           (4) *PUBLIC RECORDS.*—*Public records not other-*  
 13           *wise subject to a confidentiality or nondisclosure re-*  
 14           *quirement, or information obtained from a public*  
 15           *record, including information obtained from a news*  
 16           *report or periodical.*

17           (d) *SAFE HARBORS.*—

18           (1) *IN GENERAL.*—*A business entity shall be*  
 19           *deemed in compliance with the privacy and security*  
 20           *program requirements under section 202 if the busi-*  
 21           *ness entity complies with or provides protection equal*  
 22           *to industry standards or standards widely accepted as*  
 23           *an effective industry practice, as identified by the*  
 24           *Federal Trade Commission, that are applicable to the*  
 25           *type of sensitive personally identifiable information*

1        *involved in the ordinary course of business of such*  
 2        *business entity.*

3            (2) *LIMITATION.*—*Nothing in this subsection*  
 4        *shall be construed to permit, and nothing does permit,*  
 5        *the Federal Trade Commission to issue regulations re-*  
 6        *quiring, or according greater legal status to, the im-*  
 7        *plementation of or application of a specific technology*  
 8        *or technological specifications for meeting the require-*  
 9        *ments of this title.*

10    **SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**  
 11                                    **AND SECURITY PROGRAM.**

12        (a) *PERSONAL DATA PRIVACY AND SECURITY PRO-*  
 13        *GRAM.*—*A business entity subject to this subtitle shall com-*  
 14        *ply with the following safeguards and any other adminis-*  
 15        *trative, technical, or physical safeguards identified by the*  
 16        *Federal Trade Commission in a rulemaking process pursu-*  
 17        *ant to section 553 of title 5, United States Code, for the*  
 18        *protection of sensitive personally identifiable information:*

19            (1) *SCOPE.*—*A business entity shall implement a*  
 20        *comprehensive personal data privacy and security*  
 21        *program that includes administrative, technical, and*  
 22        *physical safeguards appropriate to the size and com-*  
 23        *plexity of the business entity and the nature and*  
 24        *scope of its activities.*

1           (2) *DESIGN.*—*The personal data privacy and se-*  
2           *curity program shall be designed to—*

3                   (A) *ensure the privacy, security, and con-*  
4                   *fidentiality of sensitive personally identifying*  
5                   *information;*

6                   (B) *protect against any anticipated*  
7                   *vulnerabilities to the privacy, security, or integ-*  
8                   *egrity of sensitive personally identifying informa-*  
9                   *tion; and*

10                  (C) *protect against unauthorized access to*  
11                  *use of sensitive personally identifying informa-*  
12                  *tion that could create a significant risk of harm*  
13                  *or fraud to any individual.*

14           (3) *RISK ASSESSMENT.*—*A business entity*  
15           *shall—*

16                   (A) *identify reasonably foreseeable internal*  
17                   *and external vulnerabilities that could result in*  
18                   *unauthorized access, disclosure, use, or alteration*  
19                   *of sensitive personally identifiable information*  
20                   *or systems containing sensitive personally identi-*  
21                   *fiable information;*

22                   (B) *assess the likelihood of and potential*  
23                   *damage from unauthorized access, disclosure,*  
24                   *use, or alteration of sensitive personally identifi-*  
25                   *able information;*



1           (C) assess the sufficiency of its policies,  
2           technologies, and safeguards in place to control  
3           and minimize risks from unauthorized access,  
4           disclosure, use, or alteration of sensitive person-  
5           ally identifiable information; and

6           (D) assess the vulnerability of sensitive per-  
7           sonally identifiable information during destruc-  
8           tion and disposal of such information, including  
9           through the disposal or retirement of hardware.

10          (4) *RISK MANAGEMENT AND CONTROL.*—Each  
11          business entity shall—

12           (A) design its personal data privacy and se-  
13           curity program to control the risks identified  
14           under paragraph (3);

15           (B) adopt measures commensurate with the  
16           sensitivity of the data as well as the size, com-  
17           plexity, and scope of the activities of the business  
18           entity that—

19           (i) control access to systems and facili-  
20           ties containing sensitive personally identifi-  
21           able information, including controls to au-  
22           thenticate and permit access only to author-  
23           ized individuals;

24           (ii) detect, record, and preserve infor-  
25           mation relevant to actual and attempted

1        *fraudulent, unlawful, or unauthorized ac-*  
2        *cess, disclosure, use, or alteration of sen-*  
3        *sitive personally identifiable information,*  
4        *including by employees and other individ-*  
5        *uals otherwise authorized to have access;*

6                *(iii) protect sensitive personally identi-*  
7        *fiable information during use, transmission,*  
8        *storage, and disposal by encryption, redac-*  
9        *tion, or access controls that are widely ac-*  
10       *cepted as an effective industry practice or*  
11       *industry standard, or other reasonable*  
12       *means (including as directed for disposal of*  
13       *records under section 628 of the Fair Credit*  
14       *Reporting Act (15 U.S.C. 1681w) and the*  
15       *implementing regulations of such Act as set*  
16       *forth in section 682 of title 16, Code of Fed-*  
17       *eral Regulations);*

18               *(iv) ensure that sensitive personally*  
19       *identifiable information is properly de-*  
20       *stroyed and disposed of, including during*  
21       *the destruction of computers, diskettes, and*  
22       *other electronic media that contain sensitive*  
23       *personally identifiable information;*

24               *(v) trace access to records containing*  
25       *sensitive personally identifiable information*

1           so that the business entity can determine  
 2           who accessed or acquired such sensitive per-  
 3           sonally identifiable information pertaining  
 4           to specific individuals; and

5           (vi) ensure that no third party or cus-  
 6           tomer of the business entity is authorized to  
 7           access or acquire sensitive personally identi-  
 8           fiable information without the business enti-  
 9           ty first performing sufficient due diligence  
 10          to ascertain, with reasonable certainty, that  
 11          such information is being sought for a valid  
 12          legal purpose; and

13          (C) establish a plan and procedures for  
 14          minimizing the amount of sensitive personally  
 15          identifiable information maintained by such  
 16          business entity, which shall provide for the reten-  
 17          tion of sensitive personally identifiable informa-  
 18          tion only as reasonably needed for the business  
 19          purposes of such business entity or as necessary  
 20          to comply with any legal obligation.

21          (b) *TRAINING*.—Each business entity subject to this  
 22          subtitle shall take steps to ensure employee training and  
 23          supervision for implementation of the data security pro-  
 24          gram of the business entity.

25          (c) *VULNERABILITY TESTING*.—

1           (1) *IN GENERAL.*—*Each business entity subject*  
 2           *to this subtitle shall take steps to ensure regular test-*  
 3           *ing of key controls, systems, and procedures of the*  
 4           *personal data privacy and security program to detect,*  
 5           *prevent, and respond to attacks or intrusions, or other*  
 6           *system failures.*

7           (2) *FREQUENCY.*—*The frequency and nature of*  
 8           *the tests required under paragraph (1) shall be deter-*  
 9           *mined by the risk assessment of the business entity*  
 10          *under subsection (a)(3).*

11          (d) *RELATIONSHIP TO CERTAIN PROVIDERS OF SERV-*  
 12          *ICES.*—*In the event a business entity subject to this subtitle*  
 13          *engages a person or entity not subject to this subtitle (other*  
 14          *than a service provider) to receive sensitive personally iden-*  
 15          *tifiable information in performing services or functions*  
 16          *(other than the services or functions provided by a service*  
 17          *provider) on behalf of and under the instruction of such*  
 18          *business entity, such business entity shall—*

19               (1) *exercise appropriate due diligence in select-*  
 20               *ing the person or entity for responsibilities related to*  
 21               *sensitive personally identifiable information, and take*  
 22               *reasonable steps to select and retain a person or enti-*  
 23               *ty that is capable of maintaining appropriate safe-*  
 24               *guards for the security, privacy, and integrity of the*

1        *sensitive personally identifiable information at issue;*  
 2        *and*

3            (2) *require the person or entity by contract to*  
 4        *implement and maintain appropriate measures de-*  
 5        *signed to meet the objectives and requirements gov-*  
 6        *erning entities subject to section 201, this section, and*  
 7        *subtitle B.*

8        (e) *PERIODIC ASSESSMENT AND PERSONAL DATA PRI-*  
 9        *VACY AND SECURITY MODERNIZATION.—Each business en-*  
 10       *tity subject to this subtitle shall on a regular basis monitor,*  
 11       *evaluate, and adjust, as appropriate its data privacy and*  
 12       *security program in light of any relevant changes in—*

13            (1) *technology;*

14            (2) *the sensitivity of personally identifiable in-*  
 15        *formation;*

16            (3) *internal or external threats to personally*  
 17        *identifiable information; and*

18            (4) *the changing business arrangements of the*  
 19        *business entity, such as—*

20                    (A) *mergers and acquisitions;*

21                    (B) *alliances and joint ventures;*

22                    (C) *outsourcing arrangements;*

23                    (D) *bankruptcy; and*

24                    (E) *changes to sensitive personally identifi-*  
 25        *able information systems.*

1       (f) *IMPLEMENTATION TIMELINE.*—Not later than 1  
 2 year after the date of enactment of this Act, a business enti-  
 3 ty subject to the provisions of this subtitle shall implement  
 4 a data privacy and security program pursuant to this sub-  
 5 title.

6 **SEC. 203. ENFORCEMENT.**

7       (a) *CIVIL PENALTIES.*—

8           (1) *IN GENERAL.*—Any business entity that vio-  
 9 lates the provisions of sections 201 or 202 shall be  
 10 subject to civil penalties of not more than \$5,000 per  
 11 violation per day while such a violation exists, with  
 12 a maximum of \$500,000 per violation.

13          (2) *INTENTIONAL OR WILLFUL VIOLATION.*—A  
 14 business entity that intentionally or willfully violates  
 15 the provisions of sections 201 or 202 shall be subject  
 16 to additional penalties in the amount of \$5,000 per  
 17 violation per day while such a violation exists, with  
 18 a maximum of an additional \$500,000 per violation.

19          (3) *PENALTY LIMITS.*—

20           (A) *IN GENERAL.*—Notwithstanding any  
 21 other provision of law, the total sum of civil pen-  
 22 alties assessed against a business entity for all  
 23 violations of the provisions of this subtitle result-  
 24 ing from the same or related acts or omissions

1        *shall not exceed \$500,000, unless such conduct is*  
 2        *found to be willful or intentional.*

3                (B) *DETERMINATIONS.*—*The determination*  
 4        *of whether a violation of a provision of this sub-*  
 5        *title has occurred, and if so, the amount of the*  
 6        *penalty to be imposed, if any, shall be made by*  
 7        *the court sitting as the finder of fact. The deter-*  
 8        *mination of whether a violation of a provision of*  
 9        *this subtitle was willful or intentional, and if so,*  
 10       *the amount of the additional penalty to be im-*  
 11       *posed, if any, shall be made by the court sitting*  
 12       *as the finder of fact.*

13               (C) *ADDITIONAL PENALTY LIMIT.*—*If a*  
 14        *court determines under subparagraph (B) that a*  
 15        *violation of a provision of this subtitle was will-*  
 16        *ful or intentional and imposes an additional*  
 17        *penalty, the court may not impose an additional*  
 18        *penalty in an amount that exceeds \$500,000.*

19               (4) *EQUITABLE RELIEF.*—*A business entity en-*  
 20        *gaged in interstate commerce that violates this section*  
 21        *may be enjoined from further violations by a United*  
 22        *States district court.*

23               (5) *OTHER RIGHTS AND REMEDIES.*—*The rights*  
 24        *and remedies available under this section are cumu-*

1        *lative and shall not affect any other rights and rem-*  
 2        *edies available under law.*

3        *(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any*  
 4        *business entity shall have the provisions of this subtitle en-*  
 5        *forced against it by the Federal Trade Commission.*

6        *(c) STATE ENFORCEMENT.—*

7                *(1) CIVIL ACTIONS.—In any case in which the*  
 8        *attorney general of a State or any State or local law*  
 9        *enforcement agency authorized by the State attorney*  
 10       *general or by State statute to prosecute violations of*  
 11       *consumer protection law, has reason to believe that an*  
 12       *interest of the residents of that State has been or is*  
 13       *threatened or adversely affected by the acts or prac-*  
 14       *tices of a business entity that violate this subtitle, the*  
 15       *State may bring a civil action on behalf of the resi-*  
 16       *dents of that State in a district court of the United*  
 17       *States of appropriate jurisdiction to—*

18                *(A) enjoin that act or practice;*

19                *(B) enforce compliance with this subtitle; or*

20                *(C) obtain civil penalties of not more than*  
 21       *\$5,000 per violation per day while such viola-*  
 22       *tions persist, up to a maximum of \$500,000 per*  
 23       *violation.*

24                *(2) PENALTY LIMITS.—*



1           (A) *IN GENERAL.*—*Notwithstanding any*  
2           *other provision of law, the total sum of civil pen-*  
3           *alties assessed against a business entity for all*  
4           *violations of the provisions of this subtitle result-*  
5           *ing from the same or related acts or omissions*  
6           *shall not exceed \$500,000, unless such conduct is*  
7           *found to be willful or intentional.*

8           (B) *DETERMINATIONS.*—*The determination*  
9           *of whether a violation of a provision of this sub-*  
10          *title has occurred, and if so, the amount of the*  
11          *penalty to be imposed, if any, shall be made by*  
12          *the court sitting as the finder of fact. The deter-*  
13          *mination of whether a violation of a provision of*  
14          *this subtitle was willful or intentional, and if so,*  
15          *the amount of the additional penalty to be im-*  
16          *posed, if any, shall be made by the court sitting*  
17          *as the finder of fact.*

18          (C) *ADDITIONAL PENALTY LIMIT.*—*If a*  
19          *court determines under subparagraph (B) that a*  
20          *violation of a provision of this subtitle was will-*  
21          *ful or intentional and imposes an additional*  
22          *penalty, the court may not impose an additional*  
23          *penalty in an amount that exceeds \$500,000.*

24          (3) *NOTICE.*—

1           (A) *IN GENERAL.*—Before filing an action  
 2           under this subsection, the attorney general of the  
 3           State involved shall provide to the Federal Trade  
 4           Commission—

5                     (i) a written notice of that action; and

6                     (ii) a copy of the complaint for that  
 7           action.

8           (B) *EXCEPTION.*—Subparagraph (A) shall  
 9           not apply with respect to the filing of an action  
 10          by an attorney general of a State under this sub-  
 11          section, if the attorney general of a State deter-  
 12          mines that it is not feasible to provide the notice  
 13          described in this subparagraph before the filing  
 14          of the action.

15          (C) *NOTIFICATION WHEN PRACTICABLE.*—In  
 16          an action described under subparagraph (B), the  
 17          attorney general of a State shall provide the  
 18          written notice and the copy of the complaint to  
 19          the Federal Trade Commission as soon after the  
 20          filing of the complaint as practicable.

21          (4) *FEDERAL TRADE COMMISSION AUTHORITY.*—  
 22          Upon receiving notice under paragraph (2), the Fed-  
 23          eral Trade Commission shall have the right to—

1           (A) move to stay the action, pending the  
2           final disposition of a pending Federal proceeding  
3           or action as described in paragraph (4);

4           (B) intervene in an action brought under  
5           paragraph (1); and

6           (C) file petitions for appeal.

7           (5) *PENDING PROCEEDINGS.*—If the Federal  
8           Trade Commission initiates a Federal civil action for  
9           a violation of this subtitle, or any regulations there-  
10          under, no attorney general of a State may bring an  
11          action for a violation of this subtitle that resulted  
12          from the same or related acts or omissions against a  
13          defendant named in the Federal civil action initiated  
14          by the Federal Trade Commission.

15          (6) *RULE OF CONSTRUCTION.*—For purposes of  
16          bringing any civil action under paragraph (1) noth-  
17          ing in this subtitle shall be construed to prevent an  
18          attorney general of a State from exercising the powers  
19          conferred on the attorney general by the laws of that  
20          State to—

21               (A) conduct investigations;

22               (B) administer oaths and affirmations; or

23               (C) compel the attendance of witnesses or  
24          the production of documentary and other evi-  
25          dence.

1           (7) *VENUE; SERVICE OF PROCESS.*—

2                   (A) *VENUE.*—Any action brought under this  
3                   subsection may be brought in the district court  
4                   of the United States that meets applicable re-  
5                   quirements relating to venue under section 1391  
6                   of title 28, United States Code.

7                   (B) *SERVICE OF PROCESS.*—In an action  
8                   brought under this subsection, process may be  
9                   served in any district in which the defendant—  
10                   (i) is an inhabitant; or  
11                   (ii) may be found.

12           (d) *NO PRIVATE CAUSE OF ACTION.*—Nothing in this  
13           subtitle establishes a private cause of action against a busi-  
14           ness entity for violation of any provision of this subtitle.

15   **SEC. 204. RELATION TO OTHER LAWS.**

16           (a) *IN GENERAL.*—No State may require any business  
17           entity subject to this subtitle to comply with any require-  
18           ments with respect to administrative, technical, and phys-  
19           ical safeguards for the protection of personal information.

20           (b) *LIMITATIONS.*—Nothing in this subtitle shall be  
21           construed to modify, limit, or supersede the operation of  
22           the Gramm-Leach-Bliley Act or its implementing regula-  
23           tions, including those adopted or enforced by States.

1           ***Subtitle B—Security Breach***  
 2                           ***Notification***

3   ***SEC. 211. NOTICE TO INDIVIDUALS.***

4           (a) *IN GENERAL.*—Any agency, or business entity en-  
 5   gaged in interstate commerce, other than a service provider,  
 6   that uses, accesses, transmits, stores, disposes of or collects  
 7   sensitive personally identifiable information shall, following  
 8   the discovery of a security breach of such information, no-  
 9   tify any resident of the United States whose sensitive per-  
 10   sonally identifiable information has been, or is reasonably  
 11   believed to have been, accessed, or acquired.

12          (b) *OBLIGATION OF OWNER OR LICENSEE.*—

13               (1) *NOTICE TO OWNER OR LICENSEE.*—Any  
 14   agency, or business entity engaged in interstate com-  
 15   merce, that uses, accesses, transmits, stores, disposes  
 16   of, or collects sensitive personally identifiable infor-  
 17   mation that the agency or business entity does not  
 18   own or license shall notify the owner or licensee of the  
 19   information following the discovery of a security  
 20   breach involving such information.

21               (2) *NOTICE BY OWNER, LICENSEE, OR OTHER*  
 22   *DESIGNATED THIRD PARTY.*—Nothing in this subtitle  
 23   shall prevent or abrogate an agreement between an  
 24   agency or business entity required to give notice  
 25   under this section and a designated third party, in-

1 *cluding an owner or licensee of the sensitive person-*  
2 *ally identifiable information subject to the security*  
3 *breach, to provide the notifications required under*  
4 *subsection (a).*

5 (3) *BUSINESS ENTITY RELIEVED FROM GIVING*  
6 *NOTICE.—A business entity obligated to give notice*  
7 *under subsection (a) shall be relieved of such obliga-*  
8 *tion if an owner or licensee of the sensitive personally*  
9 *identifiable information subject to the security breach,*  
10 *or other designated third party, provides such notifi-*  
11 *cation.*

12 (4) *SERVICE PROVIDERS.—If a service provider*  
13 *becomes aware of a security breach of data in elec-*  
14 *tronic form containing sensitive personal information*  
15 *that is owned or possessed by another business entity*  
16 *that connects to or uses a system or network provided*  
17 *by the service provider for the purpose of transmit-*  
18 *ting, routing, or providing intermediate or transient*  
19 *storage of such data, the service provider shall be re-*  
20 *quired to notify the business entity who initiated such*  
21 *connection, transmission, routing, or storage of the se-*  
22 *curity breach if the business entity can be reasonably*  
23 *identified. Upon receiving such notification from a*  
24 *service provider, the business entity shall be required*

1       to provide the notification required under subsection  
2       (a).

3       (c) *TIMELINESS OF NOTIFICATION.*—

4           (1) *IN GENERAL.*—All notifications required  
5       under this section shall be made without unreasonable  
6       delay following the discovery by the agency or busi-  
7       ness entity of a security breach.

8           (2) *REASONABLE DELAY.*—

9           (A) *IN GENERAL.*—Reasonable delay under  
10       this subsection may include any time necessary  
11       to determine the scope of the security breach, pre-  
12       vent further disclosures, conduct the risk assess-  
13       ment described in section 202(a)(3), and restore  
14       the reasonable integrity of the data system and  
15       provide notice to law enforcement when required.

16          (B) *EXTENSION.*—

17           (i) *IN GENERAL.*—Except as provided  
18       in section 212, delay of notification shall  
19       not exceed 60 days following the discovery  
20       of the security breach, unless the business  
21       entity or agency request an extension of  
22       time and the Federal Trade Commission de-  
23       termines in writing that additional time is  
24       reasonably necessary to determine the scope  
25       of the security breach, prevent further dis-

1           *closures, conduct the risk assessment, restore*  
 2           *the reasonable integrity of the data system,*  
 3           *or to provide notice to the entity designated*  
 4           *by the Secretary of Homeland Security pur-*  
 5           *suant to section 216.*

6           (ii) *APPROVAL OF REQUEST.—If the*  
 7           *Federal Trade Commission approves the re-*  
 8           *quest for delay, the agency or business enti-*  
 9           *ty may delay the time period for notifica-*  
 10          *tion for additional periods of up to 30 days.*

11          (3) *BURDEN OF PRODUCTION.—The agency,*  
 12          *business entity, owner, or licensee required to provide*  
 13          *notice under this subtitle shall, upon the request of the*  
 14          *Attorney General or the Federal Trade Commission*  
 15          *provide records or other evidence of the notifications*  
 16          *required under this subtitle, including to the extent*  
 17          *applicable, the reasons for any delay of notification.*

18          (d) *DELAY OF NOTIFICATION AUTHORIZED FOR LAW*  
 19          *ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—*

20          (1) *IN GENERAL.—If the United States Secret*  
 21          *Service or the Federal Bureau of Investigation deter-*  
 22          *mines that the notification required under this section*  
 23          *would impede a criminal investigation, or national*  
 24          *security activity, such notification shall be delayed*  
 25          *upon written notice from the United States Secret*



1     *Service or the Federal Bureau of Investigation to the*  
 2     *agency or business entity that experienced the breach.*  
 3     *The notification from the United States Secret Service*  
 4     *or the Federal Bureau of Investigation shall specify*  
 5     *in writing the period of delay requested for law en-*  
 6     *forcement or national security purposes.*

7             (2) *EXTENDED DELAY OF NOTIFICATION.*—*If the*  
 8     *notification required under subsection (a) is delayed*  
 9     *pursuant to paragraph (1), an agency or business en-*  
 10    *tity shall give notice 30 days after the day such law*  
 11    *enforcement or national security delay was invoked*  
 12    *unless a Federal law enforcement or intelligence agen-*  
 13    *cy provides written notification that further delay is*  
 14    *necessary.*

15            (3) *LAW ENFORCEMENT IMMUNITY.*—*No non-con-*  
 16    *stitutional cause of action shall lie in any court*  
 17    *against any agency for acts relating to the delay of*  
 18    *notification for law enforcement or national security*  
 19    *purposes under this subtitle.*

20            (e) *LIMITATIONS.*—*Notwithstanding any other obliga-*  
 21    *tion under this subtitle, this subtitle does not apply to the*  
 22    *following:*

23                (1) *FINANCIAL INSTITUTIONS.*—*Financial insti-*  
 24    *tutions—*

1           (A) *subject to the data security requirements*  
 2           *and standards under section 501(b) of the*  
 3           *Gramm-Leach-Bliley Act (15 U.S.C. 6801(b));*  
 4           *and*

5           (B) *subject to the jurisdiction of an agency*  
 6           *or authority described in section 505(a) of the*  
 7           *Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).*

8           (2) *HIPAA REGULATED ENTITIES.—*

9           (A) *COVERED ENTITIES.—Covered entities*  
 10           *subject to the Health Insurance Portability and*  
 11           *Accountability Act of 1996 (42 U.S.C. 1301 et*  
 12           *seq.), including the data security requirements*  
 13           *and implementing regulations of that Act.*

14           (B) *BUSINESS ENTITIES.—A Business enti-*  
 15           *ty shall be deemed in compliance with this Act*  
 16           *if the business entity—*

17                   (i) *(I) is acting as a covered entity and*  
 18                   *as a business associate, as those terms are*  
 19                   *defined under the Health Insurance Port-*  
 20                   *ability and Accountability Act of 1996 (42*  
 21                   *U.S.C. 1301 et seq.) and is in compliance*  
 22                   *with the requirements imposed under that*  
 23                   *Act and implementing regulations promul-*  
 24                   *gated under that Act; and*

1           (ii) is subject to, and currently in  
 2           compliance, with the data breach notifica-  
 3           tion, privacy and data security require-  
 4           ments under the Health Information Tech-  
 5           nology for Economic and Clinical Health  
 6           (HITECH) Act, (42 U.S.C. 17932) and im-  
 7           plementing regulations promulgated there-  
 8           under; or

9           (ii) is acting as a vendor of personal  
 10          health records and third party service pro-  
 11          vider, subject to the Health Information  
 12          Technology for Economic and Clinical  
 13          Health (HITECH) Act (42 U.S.C. 17937),  
 14          including the data breach notification re-  
 15          quirements and implementing regulations of  
 16          that Act.

17 **SEC. 212. EXEMPTIONS.**

18       (a) *EXEMPTION FOR NATIONAL SECURITY AND LAW*  
 19 *ENFORCEMENT.*—

20           (1) *IN GENERAL.*—Section 211 shall not apply to  
 21       an agency or business entity if—

22           (A) the United States Secret Service or the  
 23       Federal Bureau of Investigation determines that  
 24       notification of the security breach could be ex-  
 25       pected to reveal sensitive sources and methods or

1           *similarly impede the ability of the Government*  
 2           *to conduct law enforcement investigations; or*

3                     *(B) the Federal Bureau of Investigation de-*  
 4                     *termines that notification of the security breach*  
 5                     *could be expected to cause damage to the na-*  
 6                     *tional security.*

7           (2) *IMMUNITY.*—*No non-constitutional cause of*  
 8           *action shall lie in any court against any Federal*  
 9           *agency for acts relating to the exemption from notifi-*  
 10           *cation for law enforcement or national security pur-*  
 11           *poses under this title.*

12           (b) *SAFE HARBOR.*—

13                     (1) *IN GENERAL.*—*An agency or business entity*  
 14           *shall be exempt from the notice requirements under*  
 15           *section 211, if—*

16                     (A) *a risk assessment conducted by the*  
 17                     *agency or business entity concludes that, based*  
 18                     *upon the information available, there is no sig-*  
 19                     *nificant risk that a security breach has resulted*  
 20                     *in, or will result in, identity theft, economic loss*  
 21                     *or harm, or physical harm to the individuals*  
 22                     *whose sensitive personally identifiable informa-*  
 23                     *tion was subject to the security breach;*

24                     (B) *without unreasonable delay, but not*  
 25                     *later than 45 days after the discovery of a secu-*

1        *rity breach, unless extended by the Federal Trade*  
 2        *Commission, the agency or business entity noti-*  
 3        *fies the Federal Trade Commission, in writing,*  
 4        *of—*

5                *(i) the results of the risk assessment;*

6                *and*

7                *(ii) its decision to invoke the risk as-*  
 8                *essment exemption; and*

9                *(C) the Federal Trade Commission does not*  
 10        *indicate, in writing, within 10 business days*  
 11        *from receipt of the decision, that notice should be*  
 12        *given.*

13        *(2) REBUTTABLE PRESUMPTIONS.—For purposes*  
 14        *of paragraph (1)—*

15                *(A) the encryption of sensitive personally*  
 16        *identifiable information described in paragraph*  
 17        *(1)(A)(i) shall establish a rebuttable presumption*  
 18        *that no significant risk exists; and*

19                *(B) the rendering of sensitive personally*  
 20        *identifiable information described in paragraph*  
 21        *(1)(A)(ii) unusable, unreadable, or indecipher-*  
 22        *able through data security technology or method-*  
 23        *ology that is generally accepted by experts in the*  
 24        *field of information security, such as redaction*

1           or access controls shall establish a rebuttable pre-  
2           sumption that no significant risk exists.

3           (3) *VIOLATION.*—It shall be a violation of this  
4           section to—

5                   (A) fail to conduct the risk assessment in a  
6                   reasonable manner, or according to standards  
7                   generally accepted by experts in the field of in-  
8                   formation security; or

9                   (B) submit the results of a risk assessment  
10                  that contains fraudulent or deliberately mis-  
11                  leading information.

12          (c) *FINANCIAL FRAUD PREVENTION EXEMPTION.*—

13                  (1) *IN GENERAL.*—A business entity will be ex-  
14                  empt from the notice requirement under section 211  
15                  if the business entity utilizes or participates in a se-  
16                  curity program that—

17                          (A) effectively blocks the use of the sensitive  
18                          personally identifiable information to initiate  
19                          unauthorized financial transactions before they  
20                          are charged to the account of the individual; and

21                          (B) provides for notice to affected individ-  
22                          uals after a security breach that has resulted in  
23                          fraud or unauthorized transactions.

24                  (2) *LIMITATION.*—The exemption in paragraph

25                  (1) does not apply if the information subject to the

1       *security breach includes an individual's first and last*  
2       *name, or any other type of sensitive personally identi-*  
3       *fiable information as defined in section 3, unless that*  
4       *information is only a credit card number or credit*  
5       *card security code.*

6   **SEC. 213. METHODS OF NOTICE.**

7       *An agency or business entity shall be in compliance*  
8       *with section 211 if it provides the following:*

9           (1) *INDIVIDUAL NOTICE.—Notice to individuals*  
10          *by 1 of the following means:*

11               (A) *Written notification to the last known*  
12               *home mailing address of the individual in the*  
13               *records of the agency or business entity.*

14               (B) *Telephone notice to the individual per-*  
15               *sonally.*

16               (C) *E-mail notice, if the individual has*  
17               *consented to receive such notice and the notice is*  
18               *consistent with the provisions permitting elec-*  
19               *tronic transmission of notices under section 101*  
20               *of the Electronic Signatures in Global and Na-*  
21               *tional Commerce Act (15 U.S.C. 7001).*

22           (2) *MEDIA NOTICE.—Notice to major media out-*  
23           *lets serving a State or jurisdiction, if the number of*  
24           *residents of such State whose sensitive personally*  
25           *identifiable information was, or is reasonably believed*

1        *to have been, accessed or acquired by an unauthorized*  
 2        *person exceeds 5,000.*

3    **SEC. 214. CONTENT OF NOTIFICATION.**

4        *(a) IN GENERAL.—Regardless of the method by which*  
 5        *notice is provided to individuals under section 213, such*  
 6        *notice shall include, to the extent possible—*

7                *(1) a description of the categories of sensitive*  
 8                *personally identifiable information that was, or is*  
 9                *reasonably believed to have been, accessed or acquired*  
 10               *by an unauthorized person;*

11               *(2) a toll-free number—*

12                        *(A) that the individual may use to contact*  
 13                        *the agency or business entity, or the agent of the*  
 14                        *agency or business entity; and*

15                        *(B) from which the individual may learn*  
 16                        *what types of sensitive personally identifiable in-*  
 17                        *formation the agency or business entity main-*  
 18                        *tained about that individual; and*

19                *(3) the toll-free contact telephone numbers and*  
 20                *addresses for the major credit reporting agencies.*

21        *(b) ADDITIONAL CONTENT.—Notwithstanding section*  
 22        *219, a State may require that a notice under subsection*  
 23        *(a) shall also include information regarding victim protec-*  
 24        *tion assistance provided for by that State.*



1       (c) *DIRECT BUSINESS RELATIONSHIP.*—Regardless of  
 2 *whether a business entity, agency, or a designated third*  
 3 *party provides the notice required pursuant to section*  
 4 *211(b), such notice shall include the name of the business*  
 5 *entity or agency that has a direct relationship with the in-*  
 6 *dividual being notified.*

7       **SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT**  
 8               **REPORTING AGENCIES.**

9       *If an agency or business entity is required to provide*  
 10 *notification to more than 5,000 individuals under section*  
 11 *211(a), the agency or business entity shall also notify all*  
 12 *consumer reporting agencies that compile and maintain*  
 13 *files on consumers on a nationwide basis (as defined in sec-*  
 14 *tion 603(p) of the Fair Credit Reporting Act (15 U.S.C.*  
 15 *1681a(p)) of the timing and distribution of the notices.*  
 16 *Such notice shall be given to the consumer credit reporting*  
 17 *agencies without unreasonable delay and, if it will not*  
 18 *delay notice to the affected individuals, prior to the dis-*  
 19 *tribution of notices to the affected individuals.*

20       **SEC. 216. NOTICE TO LAW ENFORCEMENT.**

21       (a) *DESIGNATION OF GOVERNMENT ENTITY TO RE-*  
 22 *CEIVE NOTICE.*—

23               (1) *IN GENERAL.*—Not later than 60 days after  
 24 *the date of enactment of this Act, the Secretary of the*  
 25 *Department of Homeland Security shall designate a*

1 *Federal Government entity to receive the notices re-*  
 2 *quired under sections 212 and 216, and any other re-*  
 3 *ports and information about information security in-*  
 4 *cidents, threats, and vulnerabilities.*

5 (2) *RESPONSIBILITIES OF THE DESIGNATED EN-*  
 6 *TITY.—The designated entity shall—*

7 (A) *be responsible for promptly providing*  
 8 *the information that it receives to the United*  
 9 *States Secret Service and the Federal Bureau of*  
 10 *Investigation, and to the Federal Trade Commis-*  
 11 *sion for civil law enforcement purposes; and*

12 (B) *provide the information described in*  
 13 *subparagraph (A) as appropriate to other Fed-*  
 14 *eral agencies for law enforcement, national secu-*  
 15 *rity, or data security purposes.*

16 (b) *NOTICE.—Any business entity or agency shall no-*  
 17 *tify the designated entity of the fact that a security breach*  
 18 *has occurred if—*

19 (1) *the number of individuals whose sensitive*  
 20 *personally identifying information was, or is reason-*  
 21 *ably believed to have been accessed or acquired by an*  
 22 *unauthorized person exceeds 5,000;*

23 (2) *the security breach involves a database,*  
 24 *networked or integrated databases, or other data sys-*  
 25 *tem containing the sensitive personally identifiable*

1        *information of more than 500,000 individuals nation-*  
 2        *wide;*

3            *(3) the security breach involves databases owned*  
 4        *by the Federal Government; or*

5            *(4) the security breach involves primarily sen-*  
 6        *sitive personally identifiable information of individ-*  
 7        *uals known to the agency or business entity to be em-*  
 8        *ployees and contractors of the Federal Government in-*  
 9        *volved in national security or law enforcement.*

10        *(c) FTC RULEMAKING AND REVIEW OF THRESH-*  
 11        *OLDS.—Not later 1 year after the date of the enactment of*  
 12        *this Act, the Federal Trade Commission, in consultation*  
 13        *with the Attorney General of the United States and the Sec-*  
 14        *retary of the Department of Homeland Security, shall pro-*  
 15        *mulgate regulations regarding the reports required under*  
 16        *subsection (a). The Federal Trade Commission, in consulta-*  
 17        *tion with the Attorney General and the Secretary of the De-*  
 18        *partment of Homeland Security, after notice and the oppor-*  
 19        *tunity for public comment, and in a manner consistent*  
 20        *with this section, shall promulgate regulations, as nec-*  
 21        *essary, under section 553 of title 5, United States Code, to*  
 22        *adjust the thresholds for notice to law enforcement and na-*  
 23        *tional security authorities under subsection (a) and to fa-*  
 24        *cilitate the purposes of this section.*

1       (d) *TIMING.*—*The notice required under subsection (a)*  
 2 *shall be provided as promptly as possible, but such notice*  
 3 *must be provided either 72 hours before notice is provided*  
 4 *to an individual pursuant to section 211, or not later than*  
 5 *10 days after the business entity or agency discovers the*  
 6 *security breach or discovers that the nature of the security*  
 7 *breach requires notice to law enforcement under this section,*  
 8 *whichever occurs first.*

9       **SEC. 217. ENFORCEMENT.**

10       (a) *IN GENERAL.*—*The Attorney General of the United*  
 11 *States and the Federal Trade Commission may enforce civil*  
 12 *violations of section 211.*

13       (b) *CIVIL ACTIONS BY THE ATTORNEY GENERAL OF*  
 14 *THE UNITED STATES.*—

15               (1) *IN GENERAL.*—*The Attorney General may*  
 16 *bring a civil action in the appropriate United States*  
 17 *district court against any business entity that engages*  
 18 *in conduct constituting a violation of this subtitle*  
 19 *and, upon proof of such conduct by a preponderance*  
 20 *of the evidence, such business entity shall be subject*  
 21 *to a civil penalty of not more than \$11,000 per day*  
 22 *per security breach.*

23               (2) *PENALTY LIMITATION.*—*Notwithstanding any*  
 24 *other provision of law, the total amount of the civil*  
 25 *penalty assessed against a business entity for conduct*

1 *involving the same or related acts or omissions that*  
 2 *results in a violation of this subtitle may not exceed*  
 3 *\$1,000,000.*

4 (3) *DETERMINATIONS.—The determination of*  
 5 *whether a violation of a provision of this subtitle has*  
 6 *occurred, and if so, the amount of the penalty to be*  
 7 *imposed, if any, shall be made by the court sitting as*  
 8 *the finder of fact. The determination of whether a vio-*  
 9 *lation of a provision of this subtitle was willful or in-*  
 10 *tentional, and if so, the amount of the additional pen-*  
 11 *alty to be imposed, if any, shall be made by the court*  
 12 *sitting as the finder of fact.*

13 (4) *ADDITIONAL PENALTY LIMIT.—If a court de-*  
 14 *termines under paragraph (3) that a violation of a*  
 15 *provision of this subtitle was willful or intentional*  
 16 *and imposes an additional penalty, the court may not*  
 17 *impose an additional penalty in an amount that ex-*  
 18 *ceeds \$1,000,000.*

19 (c) *INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-*  
 20 *ERAL.—*

21 (1) *IN GENERAL.—If it appears that a business*  
 22 *entity has engaged, or is engaged, in any act or prac-*  
 23 *tice constituting a violation of this subtitle, the Attor-*  
 24 *ney General may petition an appropriate district*  
 25 *court of the United States for an order—*

1                   (A) enjoining such act or practice; or

2                   (B) enforcing compliance with this subtitle.

3                   (2) *ISSUANCE OF ORDER.*—A court may issue an  
4           order under paragraph (1), if the court finds that the  
5           conduct in question constitutes a violation of this sub-  
6           title.

7                   (d) *CIVIL ACTIONS BY THE FEDERAL TRADE COMMIS-*  
8           *SION.*—

9                   (1) *IN GENERAL.*—Compliance with the require-  
10          ments imposed under this subtitle may be enforced  
11          under the Federal Trade Commission Act (15 U.S.C.  
12          41 et seq.) by the Federal Trade Commission with re-  
13          spect to business entities subject to this Act. All of the  
14          functions and powers of the Federal Trade Commis-  
15          sion under the Federal Trade Commission Act are  
16          available to the Commission to enforce compliance by  
17          any person with the requirements imposed under this  
18          title.

19                  (2) *PENALTY LIMITATION.*—

20                  (A) *IN GENERAL.*—Notwithstanding any  
21          other provision of law, the total sum of civil pen-  
22          alties assessed against a business entity for all  
23          violations of the provisions of this subtitle result-  
24          ing from the same or related acts or omissions

1           *may not exceed \$1,000,000, unless such conduct*  
 2           *is found to be willful or intentional.*

3           *(B) DETERMINATIONS.—The determination*  
 4           *of whether a violation of a provision of this sub-*  
 5           *title has occurred, and if so, the amount of the*  
 6           *penalty to be imposed, if any, shall be made by*  
 7           *the court sitting as the finder of fact. The deter-*  
 8           *mination of whether a violation of a provision of*  
 9           *this subtitle was willful or intentional, and if so,*  
 10           *the amount of the additional penalty to be im-*  
 11           *posed, if any, shall be made by the court sitting*  
 12           *as the finder of fact.*

13           *(C) ADDITIONAL PENALTY LIMIT.—If a*  
 14           *court determines under subparagraph (B) that a*  
 15           *violation of a provision of this subtitle was will-*  
 16           *ful or intentional and imposes an additional*  
 17           *penalty, the court may not impose an additional*  
 18           *penalty in an amount that exceeds \$1,000,000.*

19           *(3) UNFAIR OR DECEPTIVE ACTS OR PRAC-*  
 20           *TICES.—For the purpose of the exercise by the Federal*  
 21           *Trade Commission of its functions and powers under*  
 22           *the Federal Trade Commission Act, a violation of any*  
 23           *requirement or prohibition imposed under this title*  
 24           *shall constitute an unfair or deceptive act or practice*  
 25           *in commerce in violation of a regulation under sec-*

tion 18(a)(1)(B) of the Federal Trade Commission Act ( 15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—Before opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this Act, not later than 180 days after the enactment of this Act, the Attorney General and the Commission shall enter into an agreement for coordination regarding the enforcement of this Act.



1           (B) *REQUIREMENT.*—*The coordination*  
 2           *agreement entered into under subparagraph (A)*  
 3           *shall include provisions to ensure that parallel*  
 4           *investigations and proceedings under this section*  
 5           *are conducted in a matter that avoids conflicts*  
 6           *and does not impede the ability of the Attorney*  
 7           *General to prosecute violations of Federal crimi-*  
 8           *nal laws.*

9           (4) *COORDINATION WITH THE FCC.*—*If an en-*  
 10          *forcement action under this Act relates to customer*  
 11          *proprietary network information, the Federal Trade*  
 12          *Commission shall coordinate the enforcement action*  
 13          *with the Federal Communications Commission.*

14          (f) *RULEMAKING.*—*The Federal Trade Commission*  
 15          *may, in consultation with the Attorney General, issue such*  
 16          *other regulations as it determines to be necessary to carry*  
 17          *out this subtitle. All regulations promulgated under this Act*  
 18          *shall be issued in accordance with section 553 of title 5,*  
 19          *United States Code. Where regulations relate to customer*  
 20          *proprietary network information, the promulgation of such*  
 21          *regulations will be coordinated with the Federal Commu-*  
 22          *nications Commission.*

23          (g) *OTHER RIGHTS AND REMEDIES.*—*The rights and*  
 24          *remedies available under this subtitle are cumulative and*

1 *shall not affect any other rights and remedies available*  
 2 *under law.*

3 *(h) FRAUD ALERT.—Section 605A(b)(1) of the Fair*  
 4 *Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended*  
 5 *by inserting “, or evidence that the consumer has received*  
 6 *notice that the consumer’s financial information has or*  
 7 *may have been compromised,” after “identity theft report”.*

8 **SEC. 218. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

9 *(a) IN GENERAL.—*

10 *(1) CIVIL ACTIONS.—In any case in which the*  
 11 *attorney general of a State or any State or local law*  
 12 *enforcement agency authorized by the State attorney*  
 13 *general or by State statute to prosecute violations of*  
 14 *consumer protection law, has reason to believe that an*  
 15 *interest of the residents of that State has been or is*  
 16 *threatened or adversely affected by the engagement of*  
 17 *a business entity in a practice that is prohibited*  
 18 *under this subtitle, the State or the State or local law*  
 19 *enforcement agency on behalf of the residents of the*  
 20 *agency’s jurisdiction, may bring a civil action on be-*  
 21 *half of the residents of the State or jurisdiction in a*  
 22 *district court of the United States of appropriate ju-*  
 23 *risdiction to—*

24 *(A) enjoin that practice;*

25 *(B) enforce compliance with this subtitle; or*

1           (C) *civil penalties of not more than \$11,000*  
 2           *per day per security breach up to a maximum*  
 3           *of \$1,000,000 per violation, unless such conduct*  
 4           *is found to be willful or intentional.*

5           (2) *PENALTY LIMITATION.*—

6           (A) *IN GENERAL.*—*Notwithstanding any*  
 7           *other provision of law, the total sum of civil pen-*  
 8           *alties assessed against a business entity for all*  
 9           *violations of the provisions of this subtitle result-*  
 10          *ing from the same or related acts or omissions*  
 11          *may not exceed \$1,000,000, unless such conduct*  
 12          *is found to be willful or intentional.*

13          (B) *DETERMINATIONS.*—*The determination*  
 14          *of whether a violation of a provision of this sub-*  
 15          *title has occurred, and if so, the amount of the*  
 16          *penalty to be imposed, if any, shall be made by*  
 17          *the court sitting as the finder of fact. The deter-*  
 18          *mination of whether a violation of a provision of*  
 19          *this subtitle was willful or intentional, and if so,*  
 20          *the amount of the additional penalty to be im-*  
 21          *posed, if any, shall be made by the court sitting*  
 22          *as the finder of fact.*

23          (C) *ADDITIONAL PENALTY LIMIT.*—*If a*  
 24          *court determines under subparagraph (B) that a*  
 25          *violation of a provision of this subtitle was will-*

ful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds \$1,000,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

1       (b) *FEDERAL PROCEEDINGS.*—Upon receiving notice  
 2 under subsection (a)(2), the Attorney General shall have the  
 3 right to—

4           (1) move to stay the action, pending the final  
 5 disposition of a pending Federal proceeding or action;

6           (2) initiate an action in the appropriate United  
 7 States district court under section 217 and move to  
 8 consolidate all pending actions, including State ac-  
 9 tions, in such court;

10          (3) intervene in an action brought under sub-  
 11 section (a)(2); and

12          (4) file petitions for appeal.

13       (c) *PENDING PROCEEDINGS.*—If the Attorney General  
 14 or the Federal Trade Commission initiate a criminal pro-  
 15 ceeding or civil action for a violation of a provision of this  
 16 subtitle, or any regulations thereunder, no attorney general  
 17 of a State may bring an action for a violation of a provi-  
 18 sion of this subtitle against a defendant named in the Fed-  
 19 eral criminal proceeding or civil action.

20       (d) *CONSTRUCTION.*—For purposes of bringing any  
 21 civil action under subsection (a), nothing in this subtitle  
 22 regarding notification shall be construed to prevent an at-  
 23 torney general of a State from exercising the powers con-  
 24 ferred on such attorney general by the laws of that State  
 25 to—

- 1           (1) *conduct investigations;*
- 2           (2) *administer oaths or affirmations; or*
- 3           (3) *compel the attendance of witnesses or the*
- 4           *production of documentary and other evidence.*

5           (e) *VENUE; SERVICE OF PROCESS.—*

- 6           (1) *VENUE.—Any action brought under sub-*
- 7           *section (a) may be brought in—*

8                   (A) *the district court of the United States*

9                   *that meets applicable requirements relating to*

10                  *venue under section 1391 of title 28, United*

11                  *States Code; or*

12                  (B) *another court of competent jurisdiction.*

- 13           (2) *SERVICE OF PROCESS.—In an action brought*
- 14           *under subsection (a), process may be served in any*
- 15           *district in which the defendant—*

16                   (A) *is an inhabitant; or*

17                   (B) *may be found.*

18           (f) *NO PRIVATE CAUSE OF ACTION.—Nothing in this*

19           *subtitle establishes a private cause of action against a busi-*

20           *ness entity for violation of any provision of this subtitle.*

21   **SEC. 219. EFFECT ON FEDERAL AND STATE LAW.**

22           *For any entity, or agency that is subject to this sub-*

23           *title, the provisions of this subtitle shall supersede any other*

24           *provision of Federal law, or any provisions of the law of*

25           *any State, relating to notification of a security breach, ex-*

1 *cept as provided in section 214(b). Nothing in this subtitle*  
 2 *shall be construed to modify, limit, or supersede the oper-*  
 3 *ation of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et*  
 4 *seq.) or its implementing regulations, including those regu-*  
 5 *lations adopted or enforced by States, the Health Insurance*  
 6 *Portability and Accountability Act of 1996 (42 U.S.C. 1301*  
 7 *et seq.) or its implementing regulations, or the Health In-*  
 8 *formation Technology for Economic and Clinical Health*  
 9 *Act (42 U.S.C. 17937) or its implementing regulations.*

10 **SEC. 220. REPORTING ON EXEMPTIONS.**

11 *(a) FTC REPORT.—Not later than 18 months after the*  
 12 *date of enactment of this Act, and upon request by Congress*  
 13 *thereafter, the Federal Trade Commission shall submit a*  
 14 *report to Congress on the number and nature of the security*  
 15 *breaches described in the notices filed by those business enti-*  
 16 *ties invoking the risk assessment exemption under section*  
 17 *212(b) and their response to such notices.*

18 *(b) LAW ENFORCEMENT REPORT.—*

19 *(1) IN GENERAL.—Not later than 18 months*  
 20 *after the date of enactment of this Act, and upon the*  
 21 *request by Congress thereafter, the United States Se-*  
 22 *cret Service and Federal Bureau of Investigation shall*  
 23 *submit a report to Congress on the number and na-*  
 24 *ture of security breaches subject to the national secu-*

1        *urity and law enforcement exemptions under section*  
 2        *212(a).*

3            (2) *REQUIREMENT.*—*The report required under*  
 4        *paragraph (1) shall not include the contents of any*  
 5        *risk assessment provided to the United States Secret*  
 6        *Service and the Federal Bureau of Investigation*  
 7        *under this subtitle.*

8        **SEC. 221. EFFECTIVE DATE.**

9        *This subtitle shall take effect on the expiration of the*  
 10       *date which is 90 days after the date of enactment of this*  
 11       *Act.*

12        **TITLE III—COMPLIANCE WITH**  
 13        **STATUTORY PAY-AS-YOU-GO ACT**

14        **SEC. 301. BUDGET COMPLIANCE.**

15        *The budgetary effects of this Act, for the purpose of*  
 16        *complying with the Statutory Pay-As-You-Go Act of 2010,*  
 17        *shall be determined by reference to the latest statement titled*  
 18        *“Budgetary Effects of PAYGO Legislation” for this Act,*  
 19        *submitted for printing in the Congressional Record by the*  
 20        *Chairman of the Senate Budget Committee, provided that*  
 21        *such statement has been submitted prior to the vote on pas-*  
 22        *sage.*





**Calendar No. 181**

112<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session

**S. 1151**

**A BILL**

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

SEPTEMBER 22, 2011

Reported with an amendment